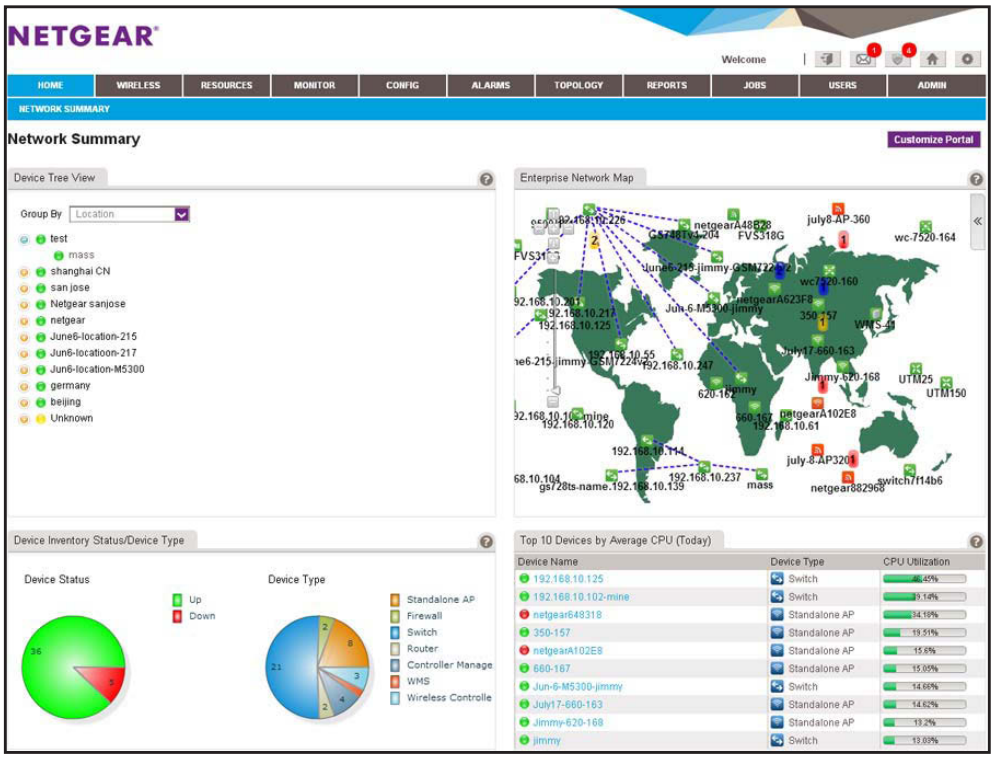
NETGEAR®

NMS300 Network Management System Application

User Manual



October 2013
202-11289-02

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates, additional documentation, and support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx.*

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved.

Revision History

Publication Part Number	Publish Date	Comments
202-11289-02	October 2013	• Revised the structure of the manual entirely. • Added support for wireless devices. • Added support for the FVS318G firewall.
202-11289-01	June 2013	First publication

Contents

Chapter 1 Introduction

Network Environment Concepts 8
Device Groups 9
Types of Users 9
Compatible Devices 10
NETGEAR Managed Switches 10
NETGEAR Smart Switches 11
NETGEAR Firewalls 12
NETGEAR Wireless Access Points 12
NETGEAR Wireless Management Systems and Controllers 12
Prepare the Network Devices for Discovery 12
What to Do Next 13

Chapter 2 Get Started

Log In to the Application 15
Change Your Password and Account Information 17
Change Your Password 17
Change Your Account Information 18
Configure the Email Server for Alerts and Alarm Notifications 19
Configure the General Email Server Settings 19
Configure Email Server Settings for a Gmail Account 21

Chapter 3 Discover and Manage Resources

Discovery Concepts 24
Use Quick Discovery to Discover Devices on Your Network 24
Use a Discovery Profile to Discover Devices on Your Network 27
Add or Modify a Device Credential 27
Add or Modify a Discovery Profile 30
Execute a Discovery Job 33
Schedule or Reschedule an Existing Discovery Job 35
Remove a Device Credential 37
Remove a Discovery Profile 38
View and Manage the Wired and Wireless Devices on Your Network 39
View Device Information 39
View Wireless Device Information Only 40
Modify the Name, Location Information, and Contact Information 43
Remove Device Information 45
Synchronize a Network Device 46
Log In to a Device 47

Ping, Perform a Traceroute, or Reboot a Device 48
Use the SNMP MIB Browser 49
View and Export the Inventory Table and Interface List Table 52
Manage Device Groups 53
Add or Modify a Static Device Group 53
Add or Modify a Dynamic Device Group 55
Remove a Device Group 56

Chapter 4 Monitor Devices and the Network

Monitor the Network 59
View the Default Network Summary 59
Customize the Network Summary Screen 61
Monitor the Top 10 Widgets for All Devices 64
View the Default Top 10 Widgets 64
Customize the Top 10 Screen 66
View the Wireless Summary and Monitor the Top 10 Widgets for Wireless Devices 71
View the Wireless Summary and Default Top 10 Wireless Widgets . . . 71
Customize the Wireless Summary Screen 73
View Device Details and Interface Details 77
Monitor Wireless Clients and View Client Details 80
Manage the Configuration Monitors 83
Configure an Individual Monitor 84
Disable a Monitor 86
Reenable a Monitor 87
View or Modify the Polling Interval for a Monitor 87
Customize the Optional Network Dashboard 88
Create or Modify a Dashboard View and Launch the Dashboard View . 88
Remove a Dashboard View 93
Customize the Network Dashboard 93
View and Export Audit Logs 95
View Firmware Version Information 95
View the NMS300 Server Information 97
View Application Notifications 98

Chapter 5 Manage Configurations and Firmware

Back Up Your Device Configurations 101
Add or Modify a Backup Profile 101
Execute a Backup Job 104
Schedule a Backup Job 105
View the Execution Status of a Backup Job 108
Remove a Backup Profile 109
Restore Your Device Configurations 110
Restore the Configuration of a Single Device 111
Customize and Promote a Configuration File 114
Promote a Configuration File for Firewalls 117
Restore the Configuration of Several Identical Devices 120

Import a Configuration File 125
Export a Configuration File 126
Modify a Configuration File 127
Remove a Configuration File 129
Compare Two Configuration Files 130
Upgrade Firmware for One or More Devices 131
Import a Firmware File 132
Execute or Schedule a Firmware Upgrade 133
Modify the File Name, Version Information, and Description for a Firmware File 137
Export a Firmware File 139
Remove a Firmware File 139

Chapter 6 Manage Alarms and Logs

View and Manage Alarms, Triggers, and Notification Profiles 142
View and Manage Current Alarms 142
View and Manage the Alarm History 144
View and Manage Alarm Configurations 146
Add a Custom Alarm Configuration 148
Modify an Alarm Configuration 150
View and Manage Alarm Notification Profiles 151
Add or Modify an Alarm Notification Profile 153
Customize Alarm Colors 156
View and Manage Network Event Notifications 157
View and Manage Device Traps 158
View and Manage Device System Logs 160

Chapter 7 Manage Maps and Topologies

View and Manage Maps 163
View a Hierarchical Map and Locate a Device 163
Manage a Hierarchical Map 165
Add a Childmap 168
Add Devices to a Map 169
Add a Link Between Devices on a Map 171
Customize the Style of a Link on a Map 174
View and Manage Network Topologies 176
Add a Topology View 176
View a Network Topology and Details About a Device 178
Manage a Topology View 181
Add a Link Between Devices on a Topology View 183
Customize the Style of a Node and Link on a Topology View 185
Remove a Topology View 188

Chapter 8 Generate and View Reports

Manage Report Templates 190
Add or Modify a Report Template 190

Remove a Report Template 194
Generate and Schedule Reports 195
Generate a One-Time Report Immediately 195
Schedule a Report 196
View and Remove Saved Reports 198
View a Saved Report 199
Remove a Saved Report 199

Chapter 9 Manage Jobs

Schedule Jobs 202
View and Manage Jobs 202

Chapter 10 Manage Users and Security Profiles

Security Profile Concepts 206
Add a Security Profile 206
Modify or Remove a Security Profile 207
Add a User Profile to the User Base 209
Modify or Remove a User Profile 210
View and Log Off Online Users 211

Chapter 11 Customize Global Settings

Set the Data Retention Period 214
Set the Inventory Polling 215
Set the Idle Time-Out 217
Set the Real-time Chart 218
Change the Auto Refresh Setting 219

Chapter 12 Manage Licenses

View License Information 222
Register a License 222
Deregister a License 223

Appendix A Technical Specifications

Appendix B Device Details

Switch Details 228
Firewall Details 229
Standalone AP Details 229
Controller-Managed AP Details 231
Wireless Controller Details 232
Wireless Managements System Details 233
Router Details 234
Unknown Device Details 234
Interface Details 235

1 Introduction

Streamline your network management tasks

The NETGEAR Network Management System 300 (NMS300) is a centralized and comprehensive management application that enables you to discover, monitor, configure, and report on enterprise-class networks with NETGEAR and third-party network devices.

This manual is intended for network administrators.

This chapter covers the following topics:

- *Network Environment Concepts*
- *Compatible Devices*
- *Prepare the Network Devices for Discovery*
- *What to Do Next*

Note: In this manual, the NMS300 application is referred to as the application. The server on which the application is installed is referred to as the NMS300 server.

For more information about the topics covered in this manual, visit the support website at *support.netgear.com*.

For more information about this NMS300 release, see the *NMS300 Release Notes*, which are available on *downloadcenter.netgear.com*.

Firmware updates with new features and bug fixes are made available from time to time on *downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

Network Environment Concepts

The application resides on the NMS300 server at a static IP address on the local area network. The application monitors the NETGEAR and third-party devices on the network.

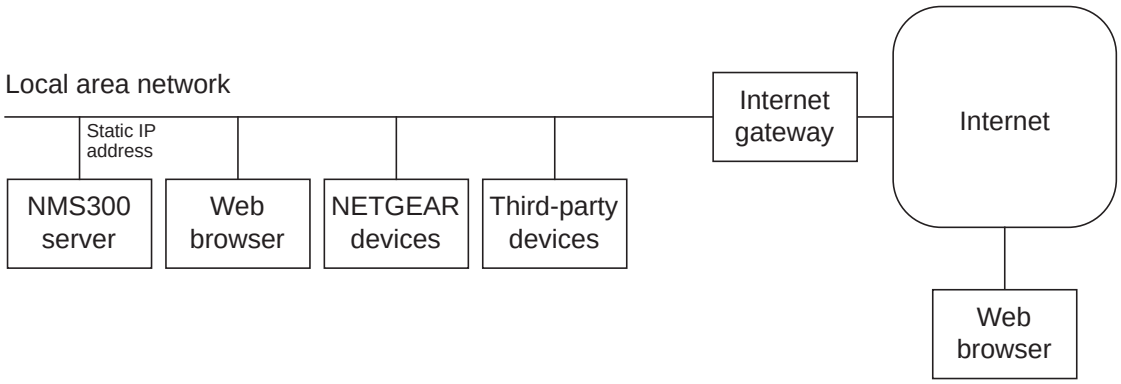


Figure 1. The Network Management System 300

You access the application through a web browser. The IP address for a web browser that is located outside the Internet gateway must have permission to access the network.

The application supports the following devices:

- NETGEAR devices

  For detailed information about the supported NETGEAR devices, including model numbers, see *Compatible Devices* on page 10.

- Third-party (non-NETGEAR) devices, including:
  - Routers
  - VoIP gateways
  - Hosts
  - Virtualization servers
- The managed NMS300 server

The application displays whether third-party devices are up or down. If a third-party device supports SNMP, the application uses SNMP MIBs to gather and present health and status information about the device.

Device Groups

To simplify the management of networks with many devices, you can create device groups. Group devices by vendor, location, device type, device model, and contact. Device groups are optional.

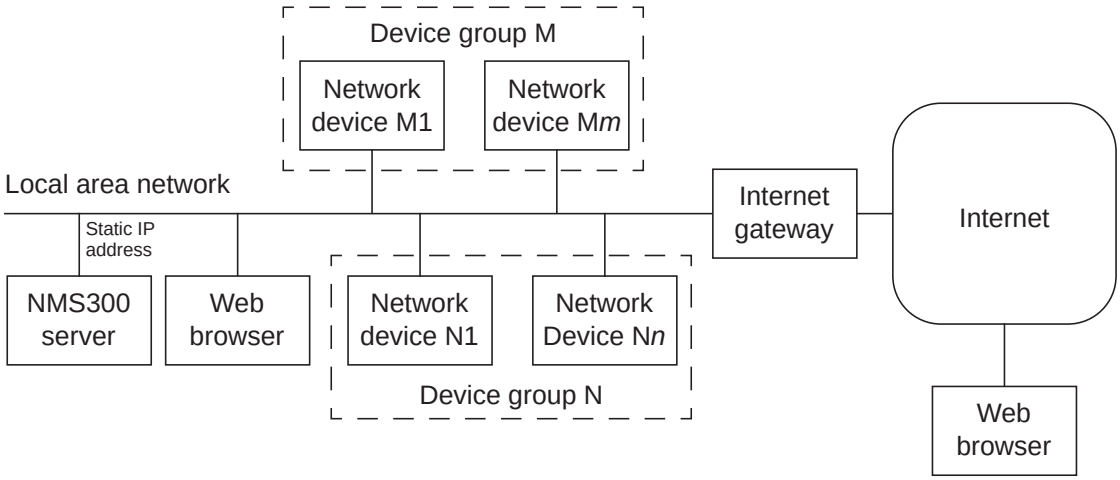


Figure 2. Device groups

You can create two types of device groups:

- **Static device groups**. A static group is a fixed list of specific devices. You must configure this list manually. For more information, see *Add or Modify a Static Device Group* on page 53.
- **Dynamic device groups**. A dynamic group is a dynamic list of devices that filter selection criteria determine. The list changes automatically as devices that meet the filter criteria are added to and removed from the network. For more information, see *Add or Modify a Dynamic Device Group* on page 55.

Types of Users

The application includes the following default user security profiles:

- **Admin**. A user with administration-related functions. An admin user has the authority to perform all application functions. Only an admin user can modify and delete the default security profiles, can define new security profiles, and can add or remove user profiles.

  For more information, see *Chapter 10, Manage Users and Security Profiles*.
- **Operator**. A user who can manage the enterprise network functions, but cannot perform administration-related functions.
- **Observer**. A user who can only monitor and view enterprise network functions.

This manual is written for the admin user but also contains information that is useful for operators and observers.

Compatible Devices

This release of the application supports the following features:

- Support for NETGEAR managed and smart switches
- Support for NETGEAR wireless devices
- Support for the NETGEAR FVS318G wired firewall
- Support for discovery and node status monitoring of third-party devices

Support for NETGEAR storage devices and additional NETGEAR security devices will be available in a future release.

NETGEAR Managed Switches

This release supports the following NETGEAR managed switches:

- FSM726-300
- GSM5212P
- GSM7212F
- GSM7212P
- GSM7224-200
- GSM7224P
- GSM7228PS
- GSM7248-200
- GSM7252PS
- GSM7328FS
- GSM7328S-200
- GSM7352S-200
- JGSM7224
- M4100-12G-POE+
- M4100-12GF
- M4100-24G-POE+
- M4100-26-POE+
- M4100-26G
- M4100-26G-POE
- M4100-50-POE
- M4100-50G
- M4100-50G-POE+
- M4100-D10-POE
- M4100-D12G

- M4100-D12G-POE+
- M5300-28G
- M5300-28G-POE+
- M5300-28G3
- M5300-28GF
- M5300-52G
- M5300-52G-POE+
- M5300-52G3
- M7100 (XSM7224)
- XSM7224S

NETGEAR Smart Switches

This release supports the following NETGEAR smart switches:

- FS728TP-200
- FS752TP
- GS108T-200
- GS110TP
- GS510TP
- GS716T-200
- GS724T-300
- GS724TP
- GS724TPS
- GS724TS
- GS728TP
- GS728TPP
- GS728TPS
- GS728TS
- GS728TXS
- GS748T-400
- GS748TP
- GS748TPS
- GS748TS
- GS752TP
- GS752TPS
- GS752TS
- GS752TXS
- XS712T

NETGEAR Firewalls

This release supports the NETGEAR FVS318G wired firewall.

NETGEAR Wireless Access Points

This release supports the following NETGEAR wireless access points:

- WG103
- WNAP210
- WNAP320
- WNDAP350
- WNDAP360
- WNDAP620
- WNDAP660

NETGEAR Wireless Management Systems and Controllers

This release supports the following NETGEAR wireless management systems and wireless controllers:

- WMS5316
- WC7520
- WC9500

Prepare the Network Devices for Discovery

To manage the devices on your network, you must prepare them for the application. By default, the application lets you manage up to 200 devices. For information about managing more than 200 devices, contact your NETGEAR sales contact.

➢ **To prepare the devices on your network:**

1. Upgrade your devices to their latest released firmware.

   To upgrade the firmware, use the web management interface of the device.

   Each device must run the latest firmware before the application can discover and manage the device. Once you perform this one-time upgrade, the application can centrally manage future device firmware upgrades.

2. Create the credentials for your devices.

   The application uses a combination of SNMP, HTTP, and Telnet protocols to interact with the devices on your network.

You must configure the application with the device credentials to authenticate with the devices over the following protocols:

- **Telnet and HTTP protocols**. If the devices do not have the default password for the admin user, create two new credentials in the application.

  Create one credential for the Telnet protocol and another credential for the HTTP protocol that contain either the admin user credential or the credential of another user of the device with administrative privileges.

- **SNMP community strings**. If the devices do not have the default SNMP community strings, create a credential in the application for the SNMP protocol that contains the matching community strings.

For more information, see *Add or Modify a Device Credential* on page 27.

3. Make sure that each device on your network is configured to send SNMPv1 or SNMPv2 traps to the IP address of the NMS300 server.

   The application listens for SNMPv1 and SNMPv2 traps.

What to Do Next

Before you can manage your network, you must perform certain basic configuration tasks and let the application find the devices that are on your network. These tasks are described in the following chapters:

- *Chapter 2, Get Started*
- *Chapter 3, Discover and Manage Resources*

2 Get Started

Log in and perform basic configuration tasks

After you have logged in to the application, you can change your password and account information and configure the email server.

This chapter covers the following topics:

- *Log In to the Application*
- *Change Your Password and Account Information*
- *Configure the Email Server for Alerts and Alarm Notifications*

Log In to the Application

The application uses a browser server architecture. Administrators and other types of users can access the application from any supported browser. For more information about installing the application, see the *NMS300 Network Management Quick Start Guide*, which is available at *downloadcenter.netgear.com*.

Before you log in to the application, check the following items:

- Make sure that the application is installed on a server with a static IP address.
- Clear your browser cache before you use the application.

CAUTION:

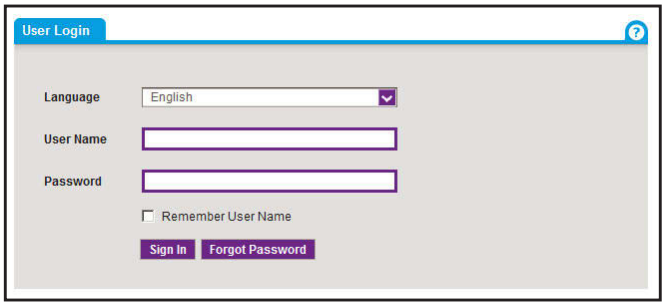
The application supports multiple concurrent users. NETGEAR recommends that different user coordinate their application activities so that modifications to a screen made by one user are not inadvertently changed by another user.

➢ **To select your language and log in to the application:**

1. Open a browser and connect to the application through the static IP address of the NMS300 server.
   - To connect to the application from the same NMS300 server on which you installed the application, enter the URL **http://localhost:8080**.

     If you entered a different port number for the NMS300 server during the application installation, replace *8080* in this URL with the port number that you provided during installation.
   - To connect to the application from a remote computer, replace *localhost* with the IP address of the NMS300 server. For example, enter **http://203.0.113.56:8080**, in which 203.0.113.56 is the IP address of the NMS300 server and 8080 is the port number for the NMS300 server.

   After you connect to the application, the User Login screen displays.



2. From the **Language** menu, select your language.

   The default language is English. You can also select Chinese.

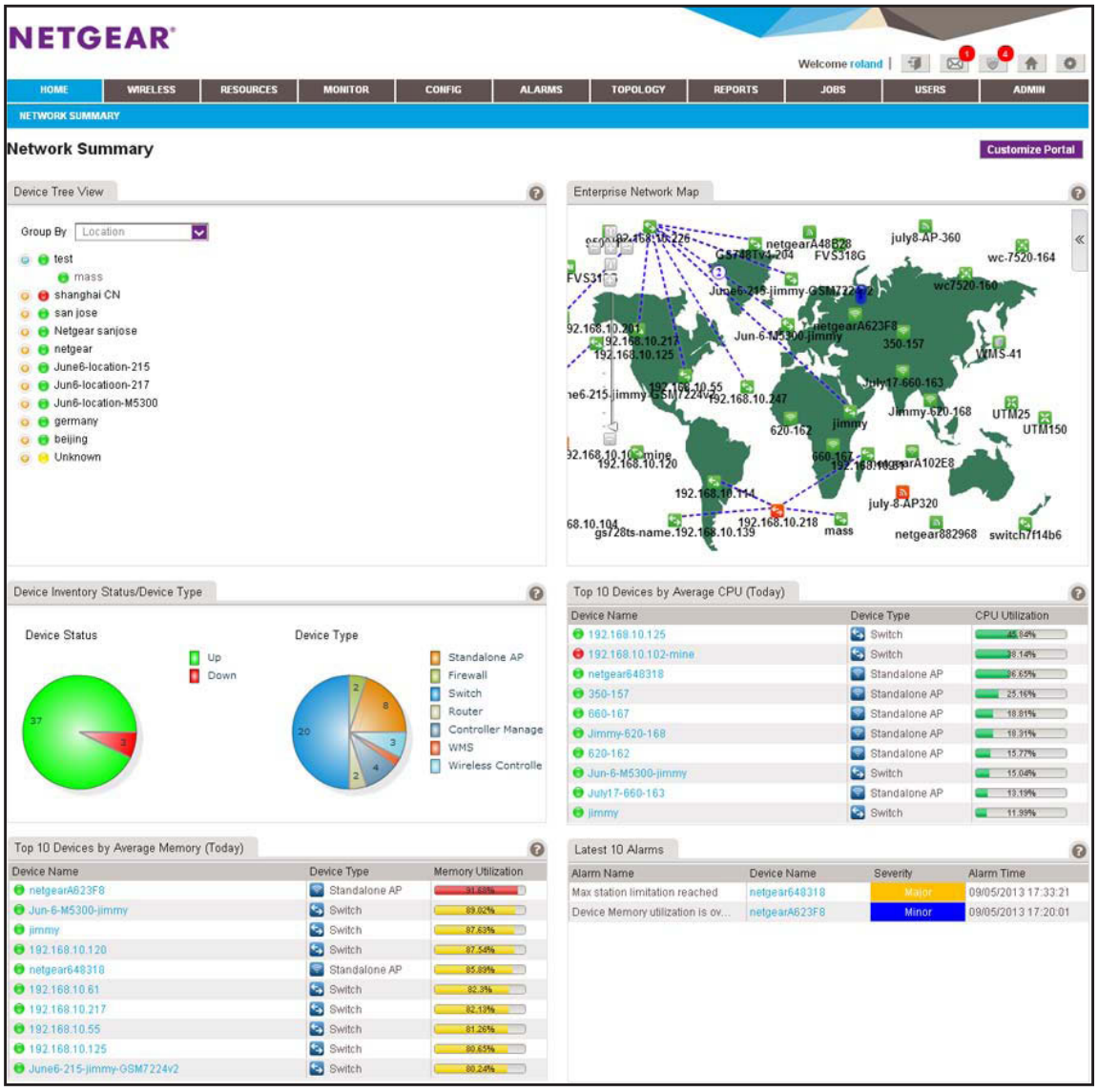
3. Enter your user name and password.

   When the application is initially installed, the default administrator user name is admin and the default administrator password is admin.

   You must be an administrator (admin user, that is, a user with a security profile that is set to Admin) to be able to create user names and passwords for other types of users.

4. Click the **Sign In** button.

   The Network Summary screen displays.



For more information about the Network Summary screen, see *Monitor the Network* on page 59.

Change Your Password and Account Information

NETGEAR recommends that you change your password to a more secure password. This recommendation applies to admin users only because nonadministrative users such as users with a security profile set to Operator or Observer cannot change their password.

As an admin user, you can also change your account information. Items that you can change include your email address, real name, and telephone number. You cannot change your user name but you can add a second admin account with a different user name. For more information, see *Chapter 10, Manage Users and Security Profiles*.

Change Your Password

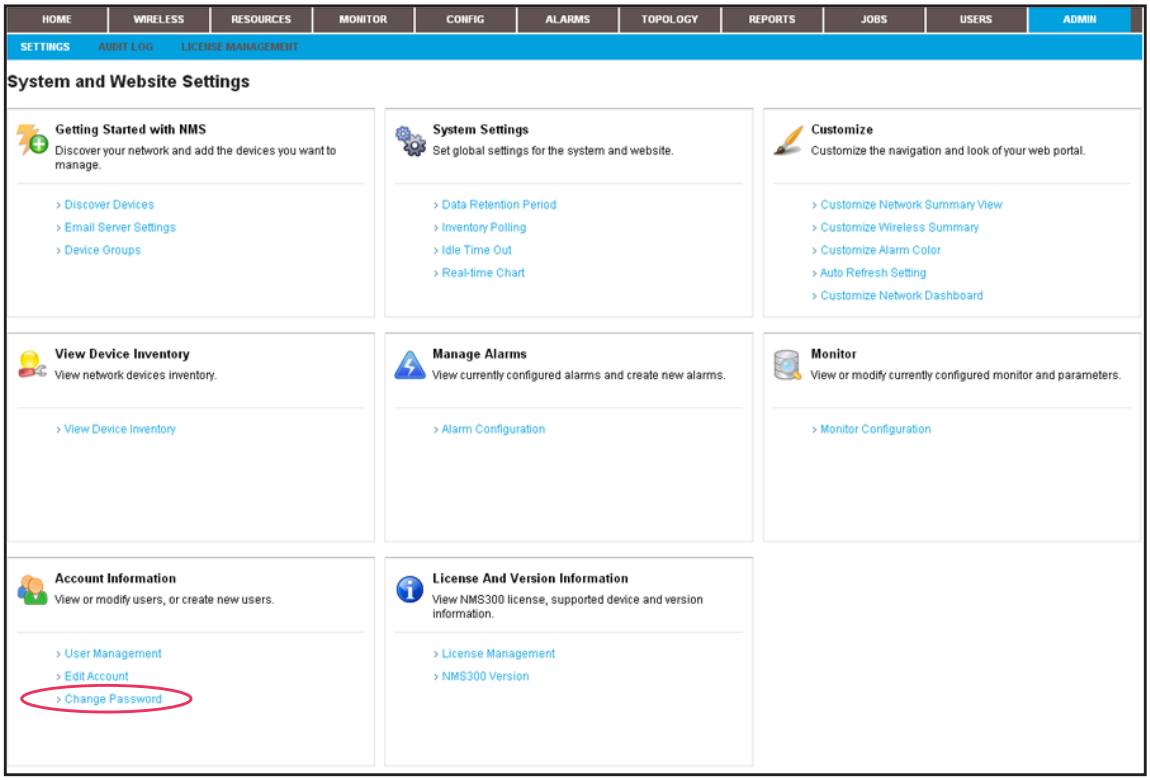
When the application is initially installed, the default administrator user name is admin and the default administrator password is admin. As an admin user, you can create user names and passwords for other types of users.

➢ **To change your password:**

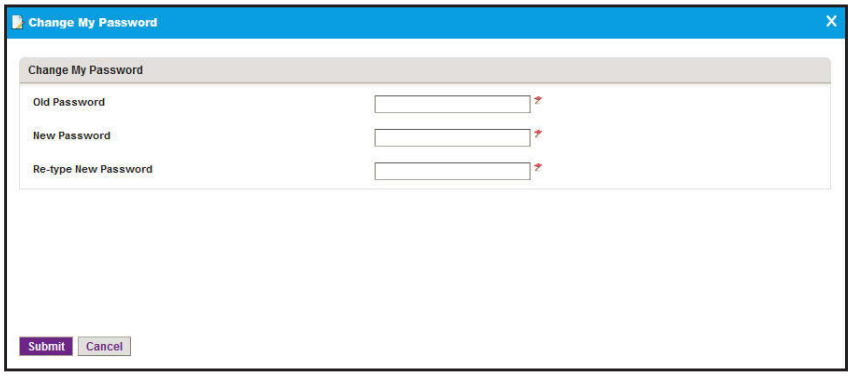
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under Account Information, click the **Change Password** link.



4. Enter your old and new passwords.
5. Click the **Submit** button.

   Your password is updated.

Change Your Account Information

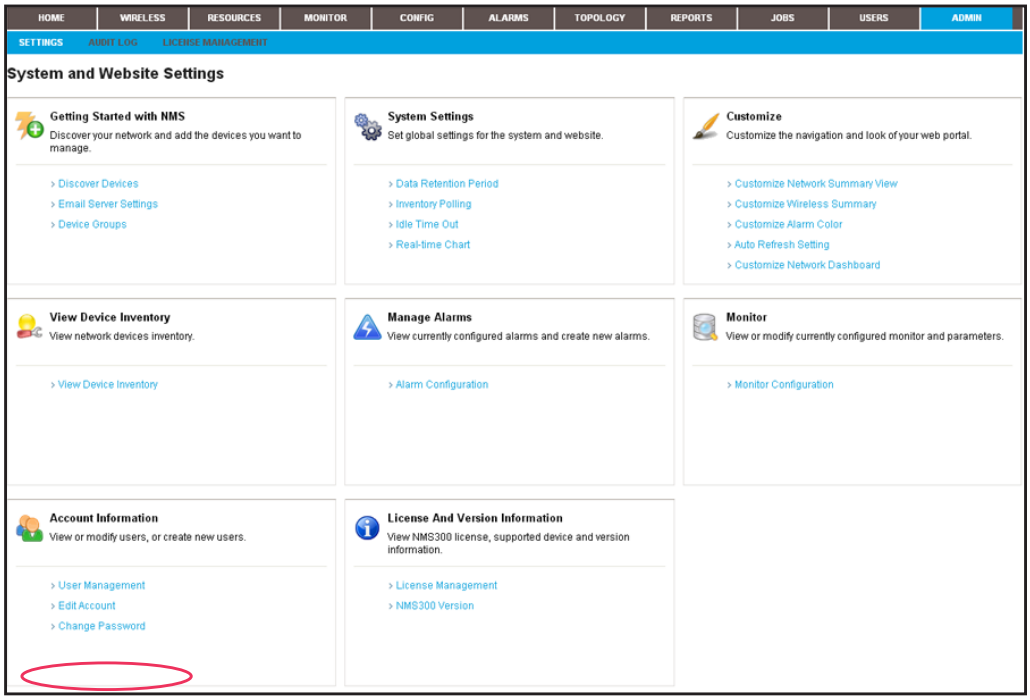
You can change your general account settings such as your email address and telephone number.

➢ **To change your account information:**

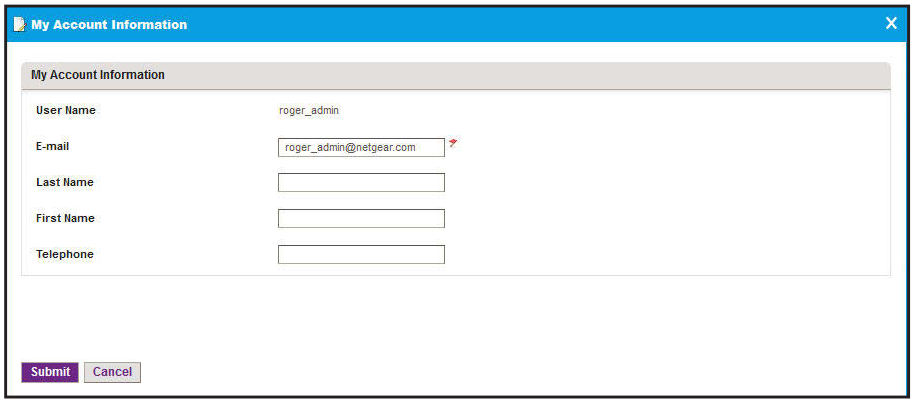
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under Account Information, click the **Edit Account** link.



4. Modify the information as needed.
5. Click the **Submit** button.

   Your account information is updated.

Configure the Email Server for Alerts and Alarm Notifications

Before the application can send email updates and alarm notifications, you must configure the email server settings. Only an admin user can configure the email server settings.

Configure the General Email Server Settings

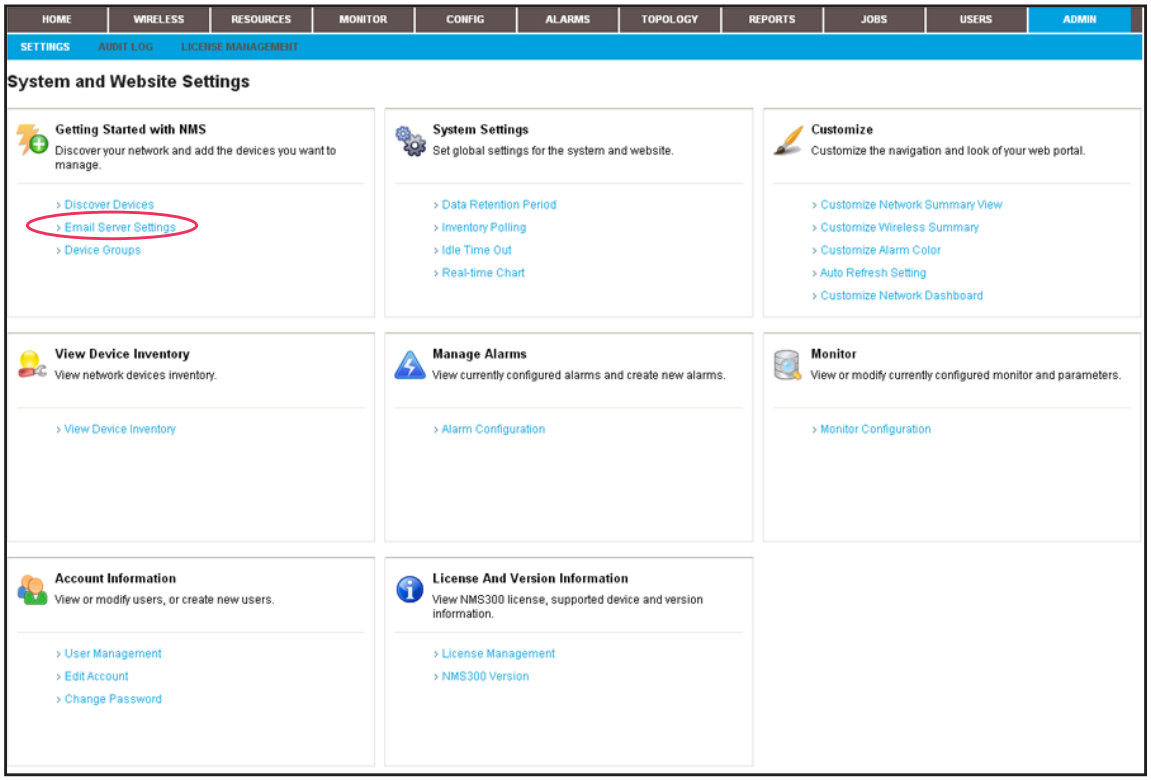
The following procedure describes how to configure the general email server Settings.

➢ **To configure the email server:**

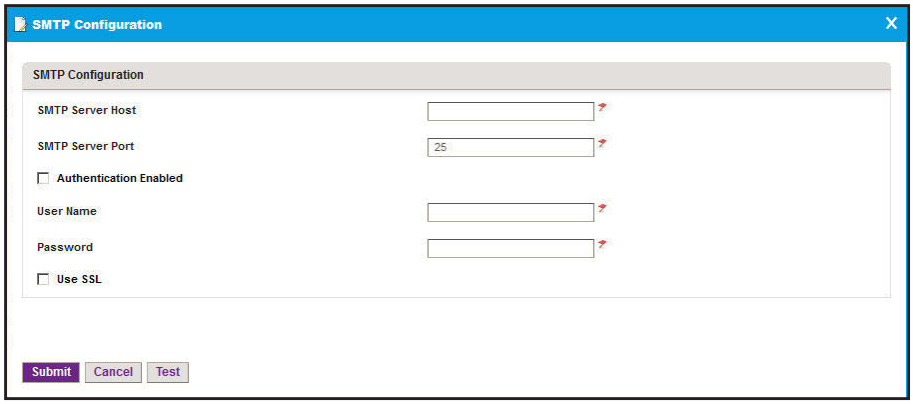
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under Getting Started with NMS, click the **Email Server Settings** link.



4. Enter your SMTP configuration settings.
5. If your SMTP server requires authentication, select the **Authentication Enabled** check box.
6. Configure the user name and password.
7. Click the **Test** button.

   Your SMTP configuration settings are verified.
8. Click the **Submit** button.

   Your changes are saved.

Configure Email Server Settings for a Gmail Account

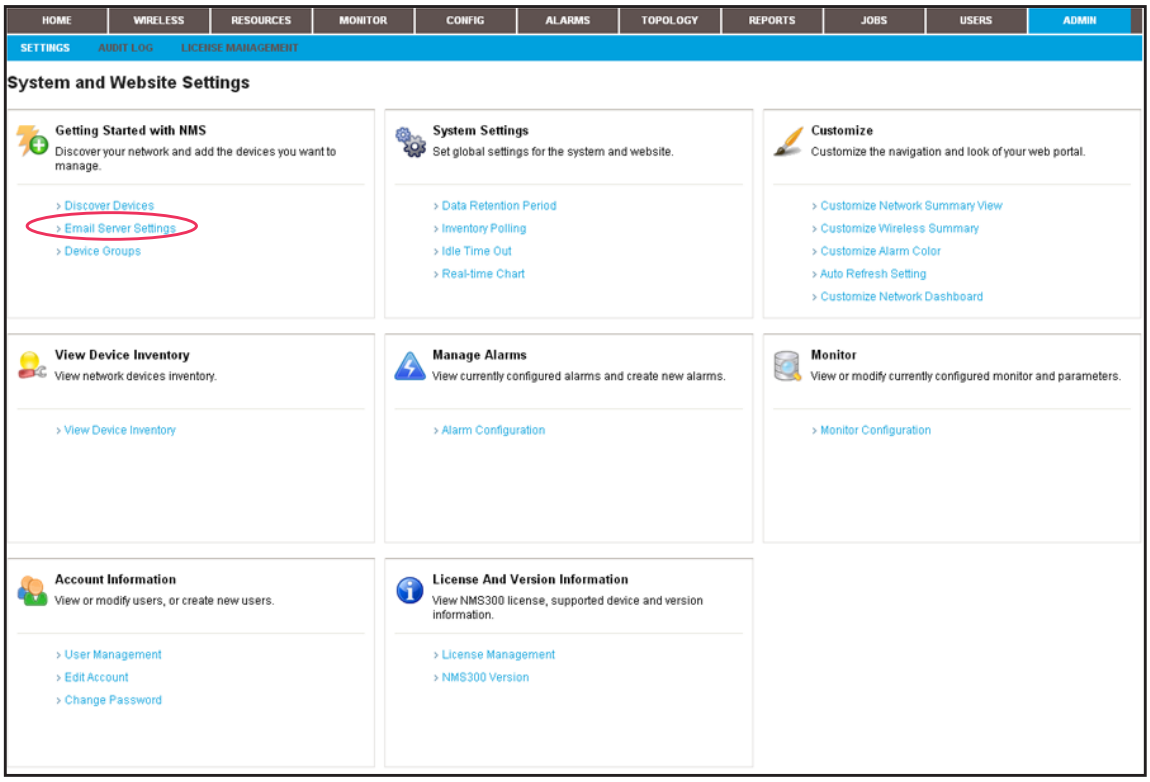
The following procedure describes how to configure the email server for a Gmail account.

➢ **To configure the email server for a Gmail account:**

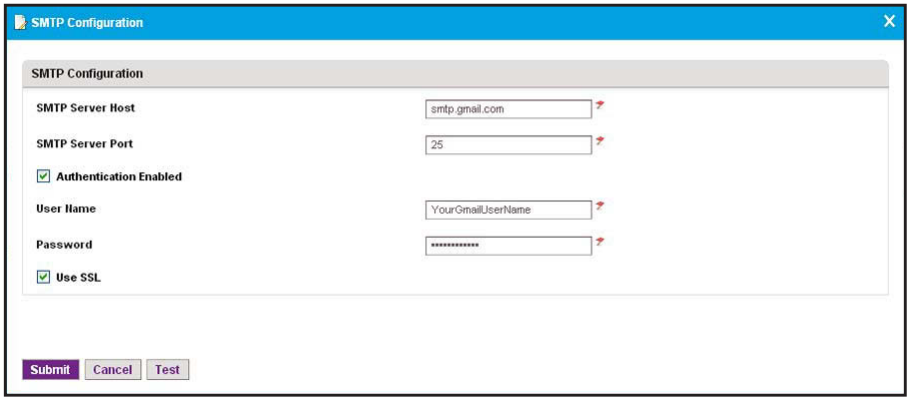
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under Getting Started with NMS, click the **Email Server Settings** link.



4. Enter the following settings and select the following check boxes:
   - In the **SMTP Server Host** field, enter **smtp.gmail.com**.
   - In the **SMPT Server Port** field, enter **25**.
   - Select the **Authentication Enabled** check box.
   - In the **User Name** field, enter the user name for your Gmail account.
   - In the **Password** field, enter the password for your Gmail account.
   - Select the **Use SSL** check box.
5. Click the **Test** button.

   Your SMTP configuration settings are verified.
6. Click the **Submit** button.

   Your changes are saved.

3 Discover and Manage Resources

Find and manage the devices on your network

Before you can manage your network, you must let the application find the devices that are on your network and perform other setup tasks that could simplify the management of your network.

This chapter covers the following topics:

- *Discovery Concepts*
- *Use Quick Discovery to Discover Devices on Your Network*
- *Use a Discovery Profile to Discover Devices on Your Network*
- *View and Manage the Wired and Wireless Devices on Your Network*
- *Manage Device Groups*

Discovery Concepts

You can discover devices on your network by using the following methods:

- **Quick discovery**. Discovers devices without using a discovery profile. This method is a quick and easy discovery method but gives you limited control over the discovery process.
- **Regular discovery**. Filters the devices on your network through a discovery profile that you must configure first. This method gives you more control than the quick discovery method but is a bit more complicated.

With both methods, the application can discover wired devices, wireless devices, NETGEAR devices, and third-party devices that support standard SNMP MIBs.

The application can discover and monitor NETGEAR firewalls over the WAN. Firewalls can have either a static WAN IP address, dynamic WAN IP address, or WAN host name. If a firewall uses a WAN host name, the firewall must have DNS enabled.

Note: By default, the application lets you discover up to 200 devices. For information about discovering more than 200 devices, contact your NETGEAR sales contact.

For wireless access points (APs), the nature of the AP determines whether the application can discover the AP:

- **Standalone AP**. An AP that is not controlled by another device and that operates in standalone mode. This type of AP is also referred to as a Fat AP. The application can discover and manage standalone APs just like any other network device that the application supports.
- **Controller-managed AP**. An AP that a NETGEAR WC7520 or WC9500 wireless controller manages. This type of AP is also referred to as a Fit AP. After the application discovers a wireless controller, it displays the controller-managed APs in the device table. In this indirect way, the application can discover the controller-managed APs but cannot manage them. You cannot back up or restore the configuration, upgrade the firmware, or delete the access points from the application. Controller-managed APs are not subtracted from the number of devices that the license of the application supports. The license of the application ignores the controller-managed APs.

Use Quick Discovery to Discover Devices on Your Network

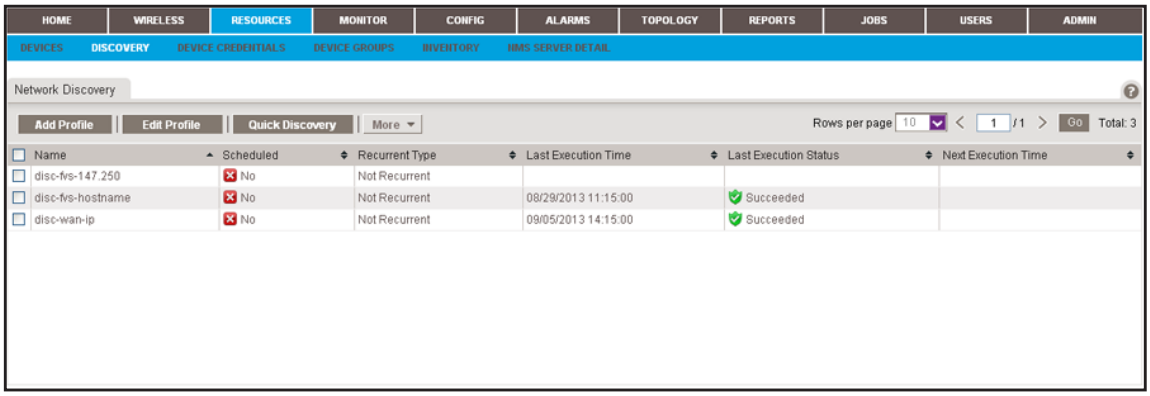
Quick Discovery is a quick and easy discovery method but gives you limited control over the discovery process.

➢ **To discover the devices on your network:**

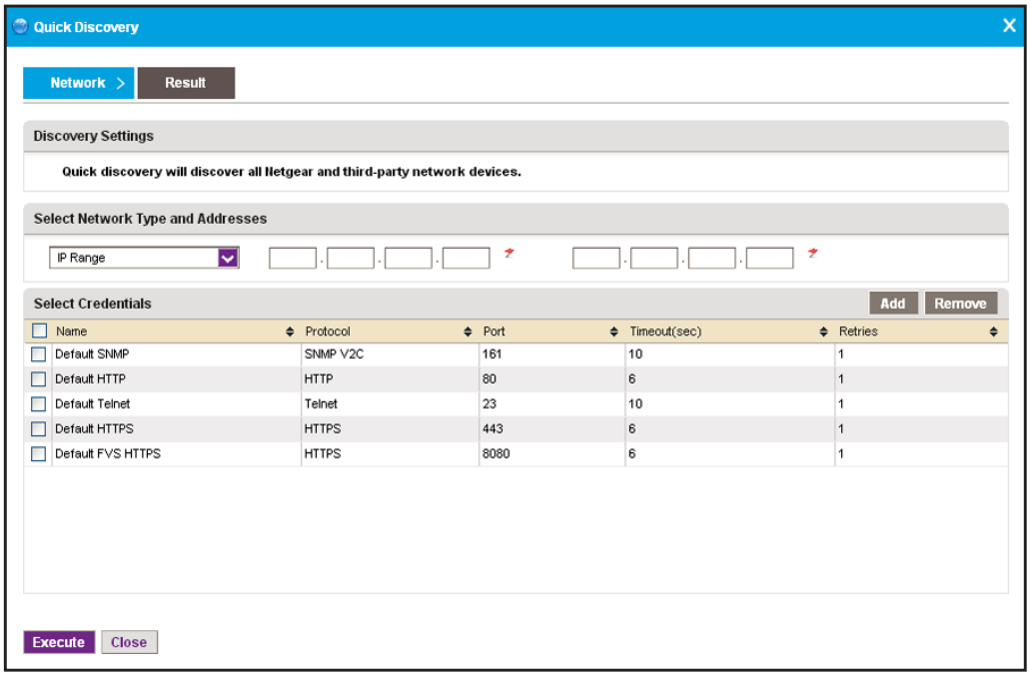
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DISCOVERY**.



3. Click the **Quick Discovery** button.



4. From the menu on the upper left of the screen, select one of the following network types and enter the applicable address information in the fields to the right of the menu:
   - **IP Range**
   - **Subnet**
   - **Single IP**
   - **IP Address(es)**
   - **Hostname**

5. Specify the credentials that pertain to the devices on your network by select one of the following types of credentials:
   - **Default SNMP**
   - **Default HTTP**
   - **Default Telnet**
   - **Default HTTPS**
   - **Default FVS HTTPS**
6. If the credential that you need is not listed in the table, do the following:
   a. Click the **Add** button.

      The Select Credentials screen displays. In addition to the default credentials, the screen displays the device credentials that you have added. For more information, see *Add or Modify a Device Credential* on page 27.

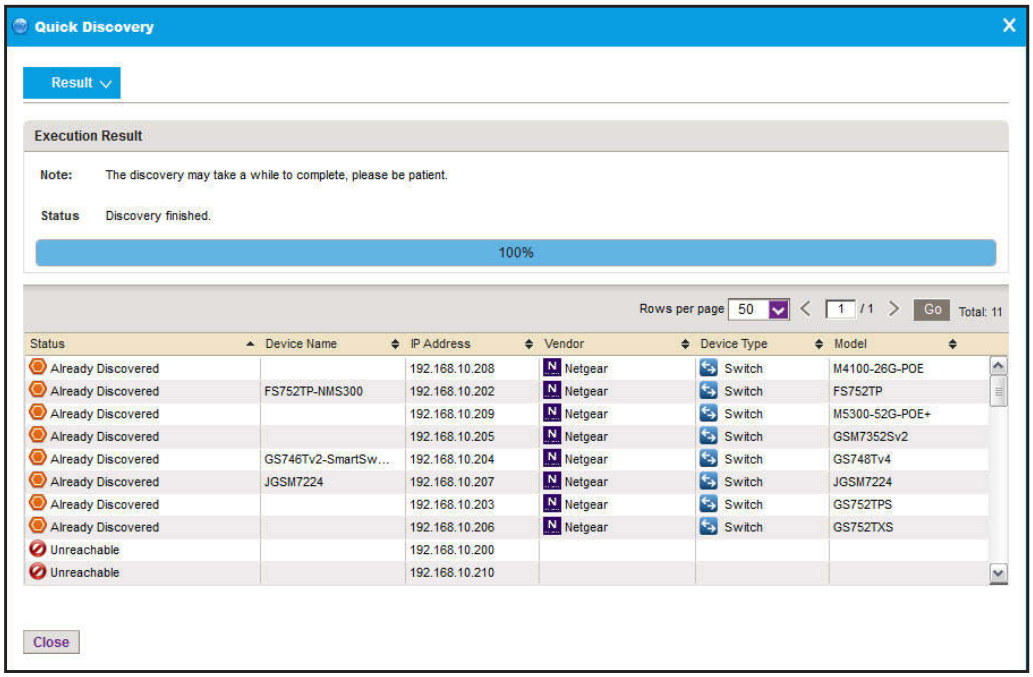
   b. Select one or more credentials and click the **Add Selection** button.

      To add all credentials, click the **Add All** button.

      The Select Credentials screen closes and the selected credentials are added to the credentials table.

   c. Select the credential or credentials that you added.
7. Click the **Execute** button.

   When the quick discovery process completes, the Quick Discovery screen displays the results.



Note: *If a credential failure occurs, a common reason is that the device login information changed from its default. When a credential failure occurs, add or modify the credential and run the discovery job again. For more information, see Add or Modify a Device Credential on page 27.*

8. Click the **Close** button.

   The Quick Discovery screen closes.

Use a Discovery Profile to Discover Devices on Your Network

A discovery profile gives you more control over the discovery process than the quick discovery method but is a bit more complicated. The following sections describe how you can use a discovery profile to discover devices:

1. *Add or Modify a Device Credential*
2. *Add or Modify a Discovery Profile*
3. *Execute a Discovery Job* or *Schedule or Reschedule an Existing Discovery Job*

Add or Modify a Device Credential

During the discovery process, the application must log in to devices to obtain the information to discover and manage the devices. A device credential includes the user name, password, and SNMP community string that allows the application to log in to the device. The user name and password are the same user information that you use to log in to the device to perform system configuration. The application provides default device credentials for discovery over HTTP, HTTPS, SNMP, and Telnet, and for discovery of the NETGEAR FVS318G firewall over HTTPS.

You must configure the correct device credentials for any device that you want the application to manage. If a device does not have its default credentials, do the following:

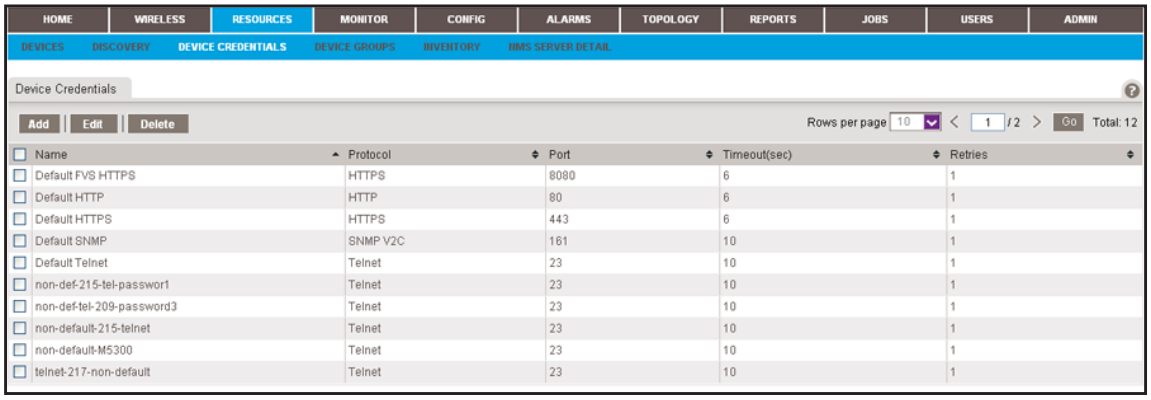
- If a device does not have its default admin user password, create two new credentials in the application, one for Telnet and another for the HTTP protocol. These credentials contain either the admin user credential or the credential of another user with administrative privileges.
- If a device does not have its default SNMP community strings, create a credential in the application for the SNMP protocol that contains the matching community strings.

➢ **To add a device credential or modify an existing device credential:**

1. Log in to the application.

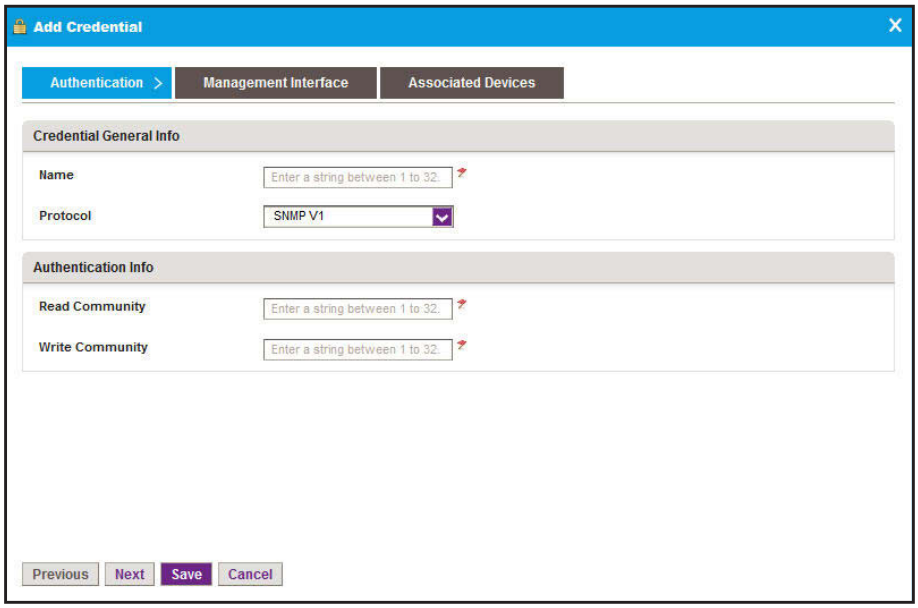
   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICE CREDENTIALS**.



3. Add a device credential or modify an existing device credential:
   - To add a device credential, click the **Add** button.
   - To modify an existing device credential:
     a. From the Device Credentials table, select a device credential.
     b. Click the **Edit** button.

   For a new device credential, the Add Credential screen displays. For an existing device credential, the Edit Credential screen displays.

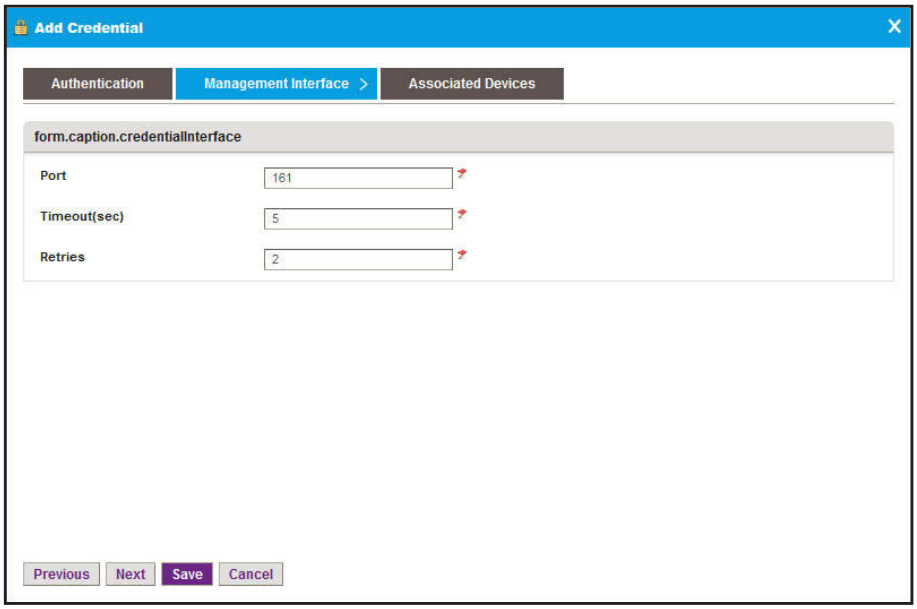


4. In the Credential General Info section, enter or modify the name for the credential.
5. From the **Protocol** menu, select one of the following protocols:
   - **SNMP V1**
   - **SNMP V2C**
   - **SNMP V3**
   - **Telnet**

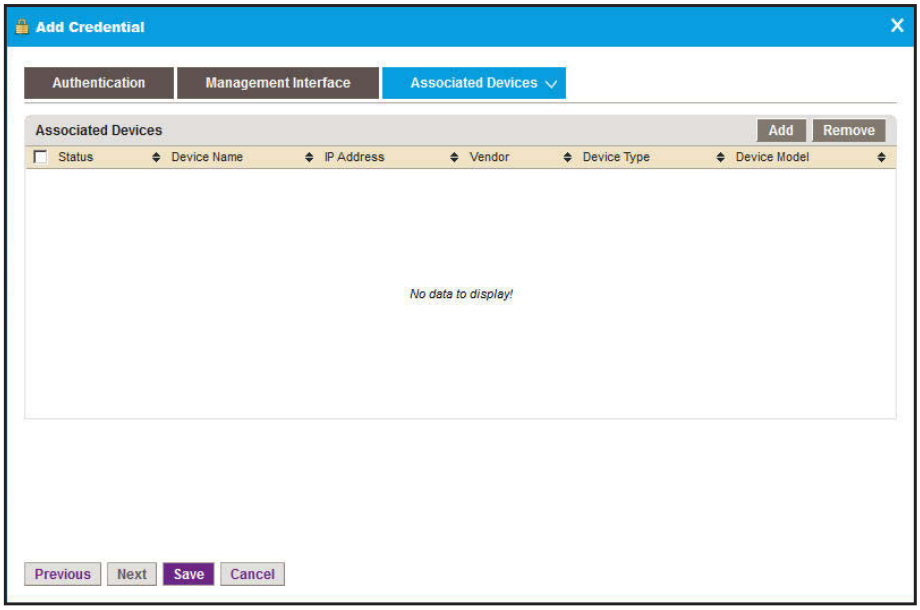
- **SSH**
- **HTTP**
- **HTTPS**

Depending on your protocol selection, the screen might adjust to display other fields and menus.

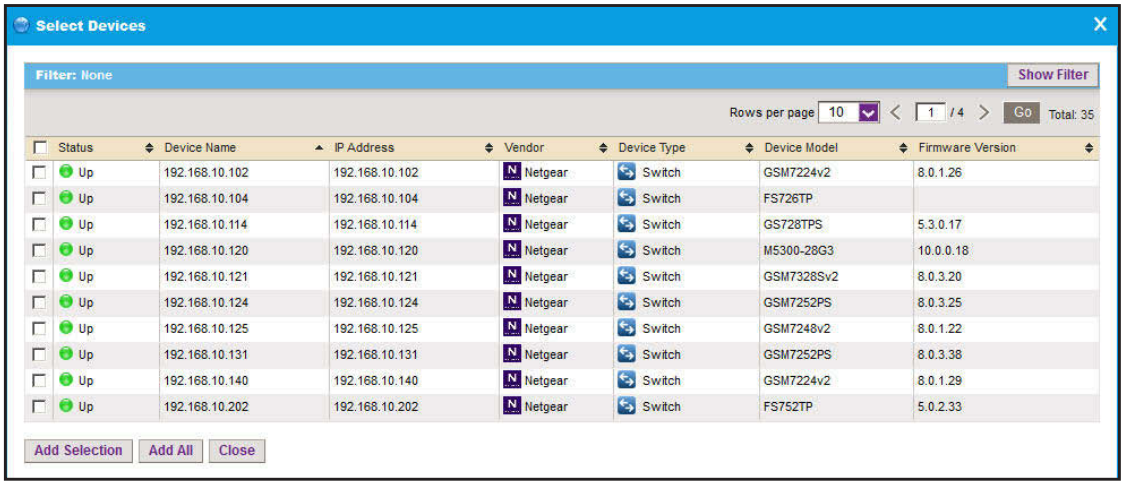
6. In the Authentication Info section, enter or modify the information for the selected protocol.
7. Click the **Management Interface** tab.



8. Enter or modify the port number, time-out period in seconds, and the number of retries.
9. Click the **Associated Devices** tab.



10. Click the **Add** button.



11. Select one or more devices and click the **Add Selection** button.

    To add all devices to the device credential, click the **Add All** button.

    The Select Devices screen closes and the selected devices are added to the Associated Devices table.

12. If you are modifying an existing device credential, to remove devices:

    a. Select the devices.

    b. Click the **Remove** button.

    The devices are removed from the Associated Devices table.

13. Click the **Save** button.

    The screen closes and the new or modified device credential displays in the Device Credentials table.

Add or Modify a Discovery Profile

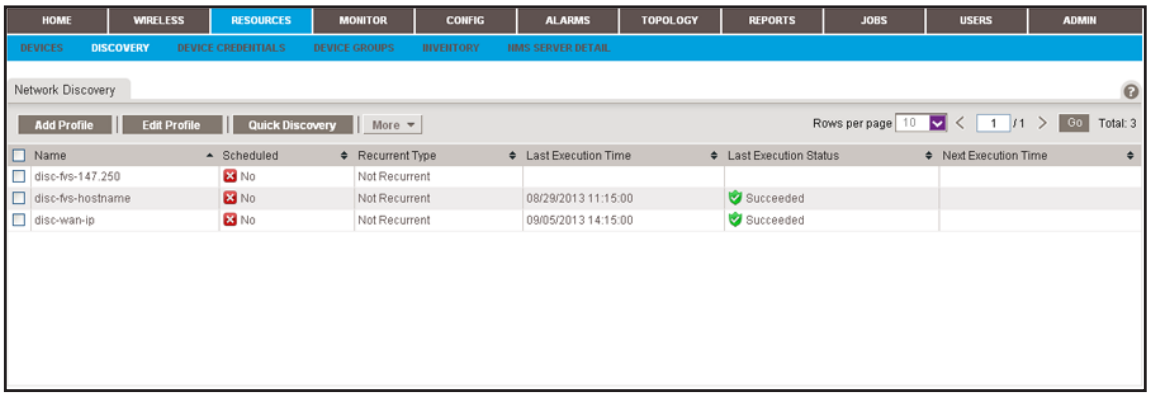
A discovery profile filters the network device information that the application can detect. The application can discover devices through an IP address range, IP subnet address, a single IP address, a list of IP addresses, or device host name.

➢ **To add a discovery profile or modify an existing discovery profile:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

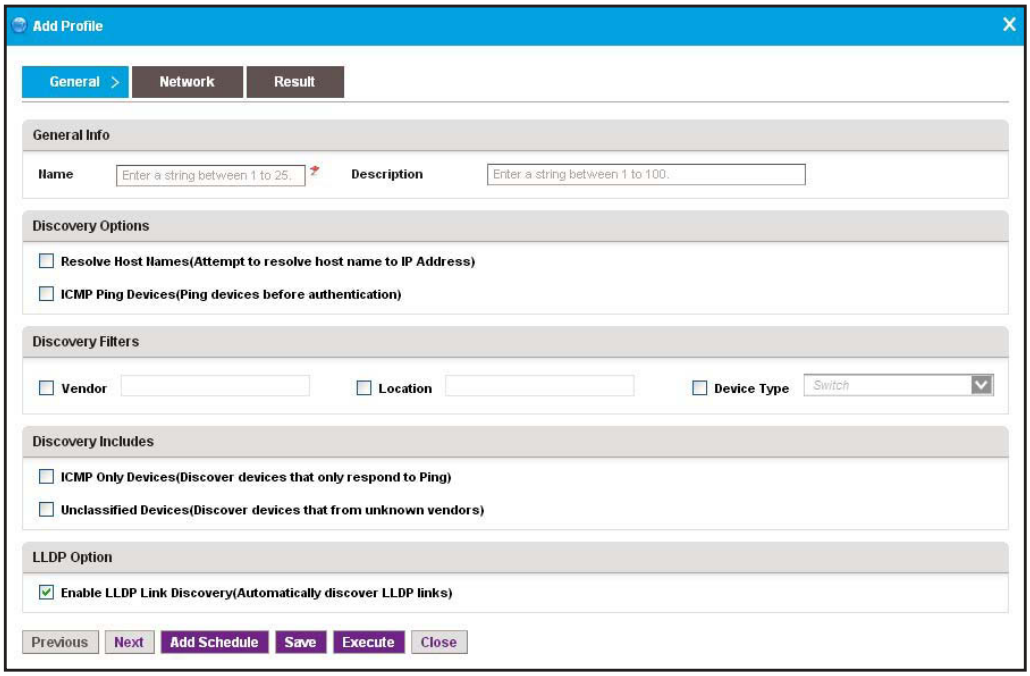
2. Select **RESOURCES > DISCOVERY**.



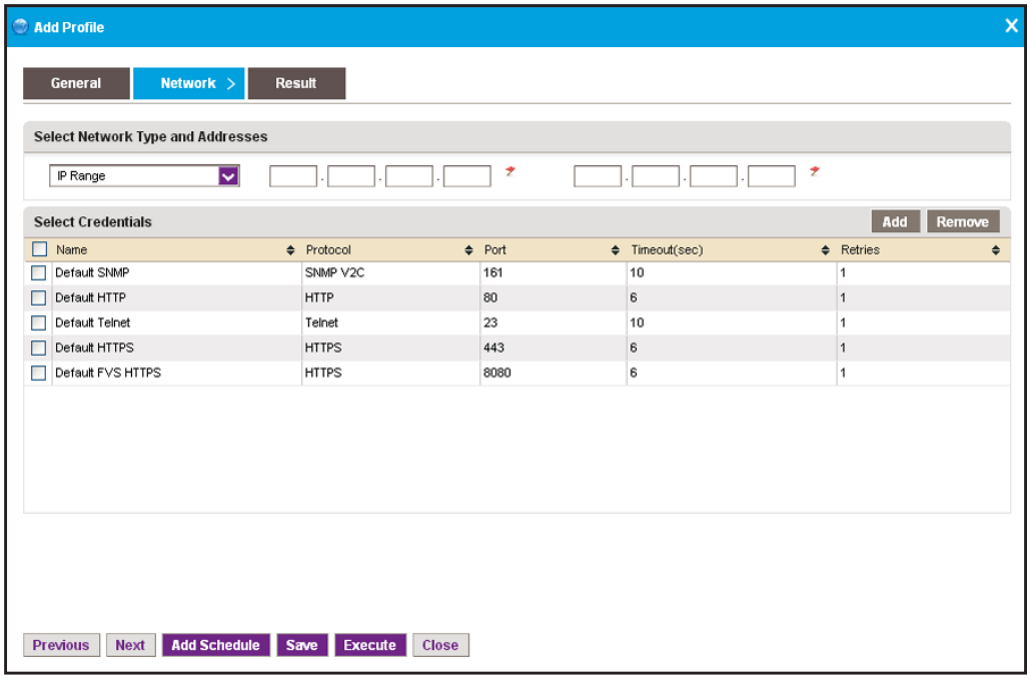
The screen displays the existing discovery profiles.

3. Add a discovery profile or modify an existing discovery profile:
   - To add a discovery profile, click the **Add Profile** button.
   - To modify an existing discovery profile:
     a. From the Network Discovery table, select a discovery profile.
     b. Click the **Edit Profile** button.

For a new discovery profile, the Add Profile screen displays. For an existing discovery profile, the Edit Profile screen displays.

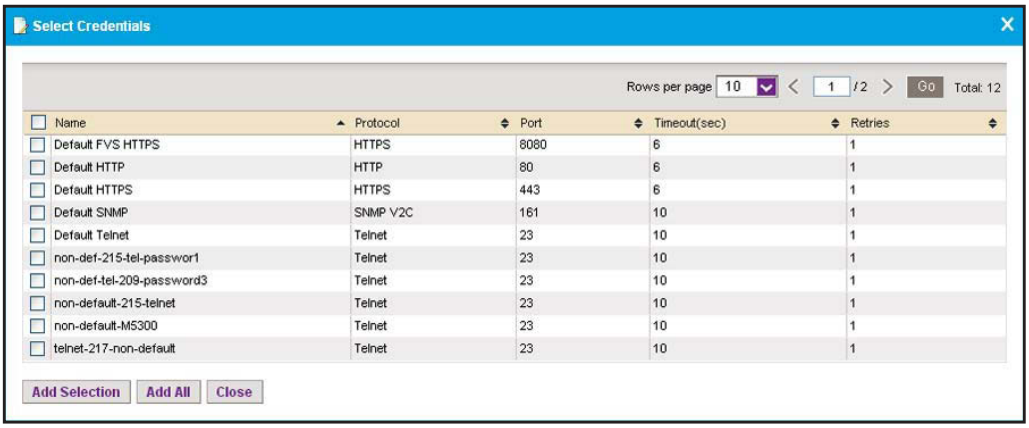


4. Enter or modify the information in the following sections:
   - **General Info**. Enter the name and description of the profile.
   - **Discovery Options**:
     - **Resolve Host Names**. To attempt to resolve a host name to an IP address, select the **Resolve Host Names (Attempt to resolve host name to IP address)** check box.
     - **ICMP Ping Devices**. To monitor the node status of third-party non-SNMP devices, select the **ICMP Ping Devices (Ping devices before authentication)** check box.
   - **Discovery Filters**. Select the discovery filters you want by vendor, location, and device type.
   - **Discovery Includes**. Select whether to include ICMP-only devices or unclassified devices.
   - **LLDP Option**. To monitor the node status of third-party non-SNMP devices, select the **Enable LLDP Link Discovery (Automatically discover LLDP links)** check box.
5. Click the **Network** tab.



6. From the menu on the upper left of the screen, select one of the following network types and enter the applicable address information in the fields to the right of the menu:
   - **IP Range**
   - **Subnet**
   - **Single IP**
   - **IP Address(es)**
   - **Hostname**

7. Specify or modify the credentials that pertain to the devices on your network by selecting one of the following types of credentials:
   - **Default SNMP**
   - **Default HTTP**
   - **Default Telnet**
   - **Default HTTPS**
   - **Default FVS HTTPS**
8. If the credential that you need is not listed in the table, do the following:
   a. Click the **Add** button.



   In addition to the default credentials, the screen displays the device credentials that you have added. For more information, see *Add or Modify a Device Credential* on page 27.

   b. Select one or more credentials and click the **Add Selection** button.

   To add all credentials, click the **Add All** button.

   The Select Credentials screen closes and the credentials are added to the Select Credentials table on the Network subscreen (the figure that is shown in *Step 5*).

   c. On the Network subscreen, select the credential or credentials that you added.
9. Click the **Save** button.

   The screen closes and the new or modified discovery profile displays in the Network Discovery table.

Execute a Discovery Job

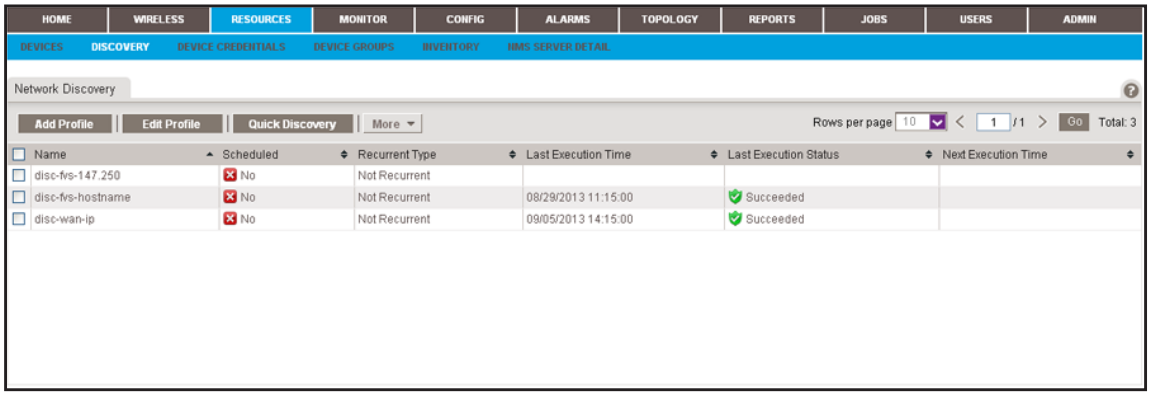
You can execute a one-time discovery job immediately.

➢ **To execute a discovery job:**

1. Log in to the application.

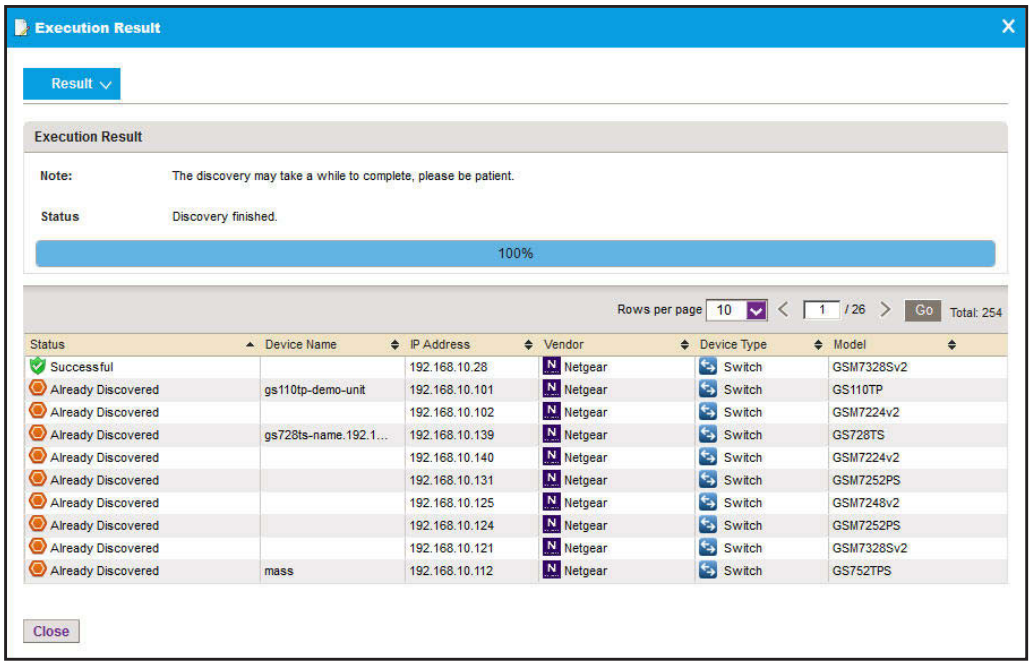
   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DISCOVERY**.



3. Select the discovery profile.
4. From the **More** menu, select **Execute**.

   When discovery completes, the Execution Results screen displays the discovered devices that the application adds to its inventory database.



5. Click the **Close** button.

   The screen closes.

Note: Output files from completed resource discovery jobs are saved for the data retention period. For more information, see *Set the Data Retention Period* on page 214.

Schedule or Reschedule an Existing Discovery Job

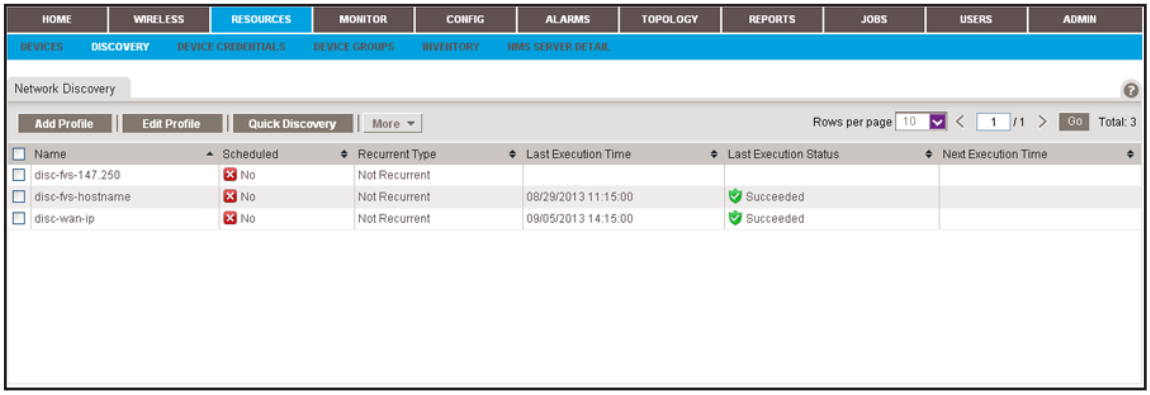
You can schedule or reschedule an existing discovery job to occur later. This discovery job can be one time or recurrent.

➢ **To schedule or reschedule an existing discovery job for future execution:**

1. Log in to the application.

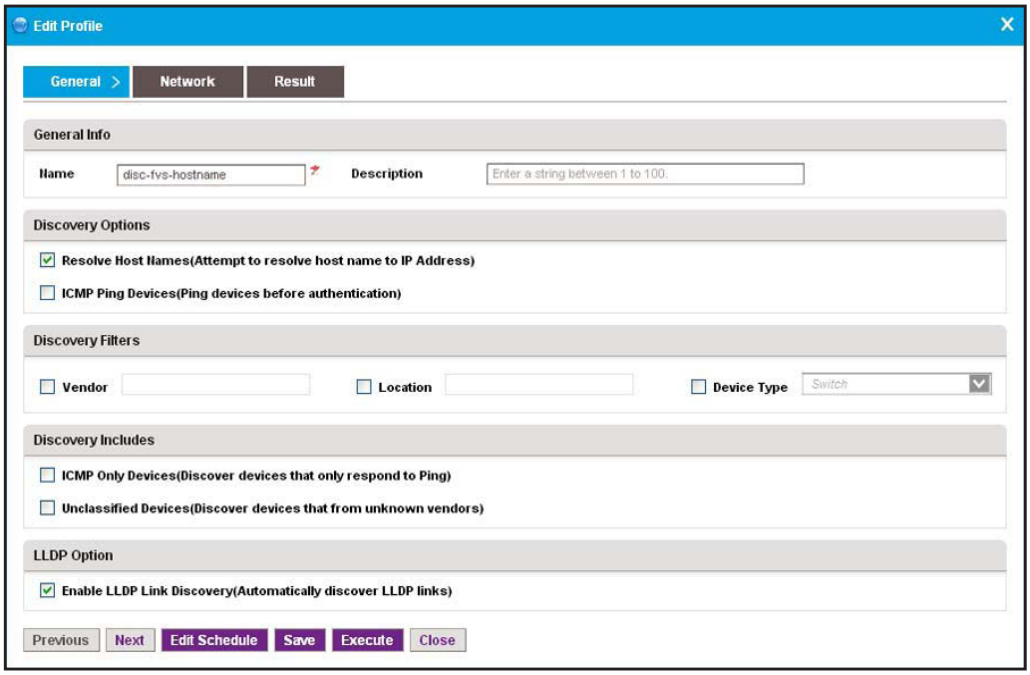
   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DISCOVERY**.

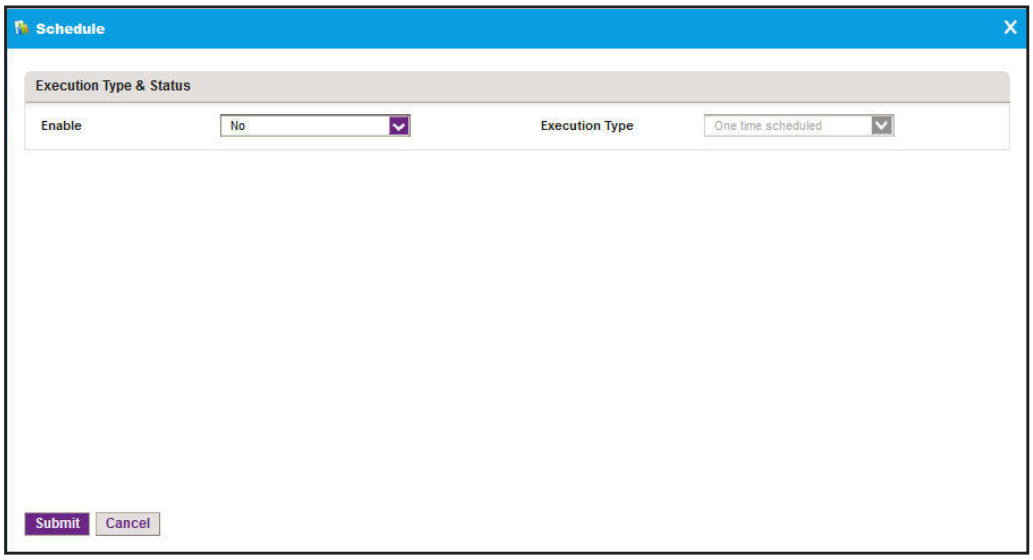


   The screen lists the existing discovery profiles in the application.

3. Select the discovery profile.
4. Click the **Edit Profile** button.

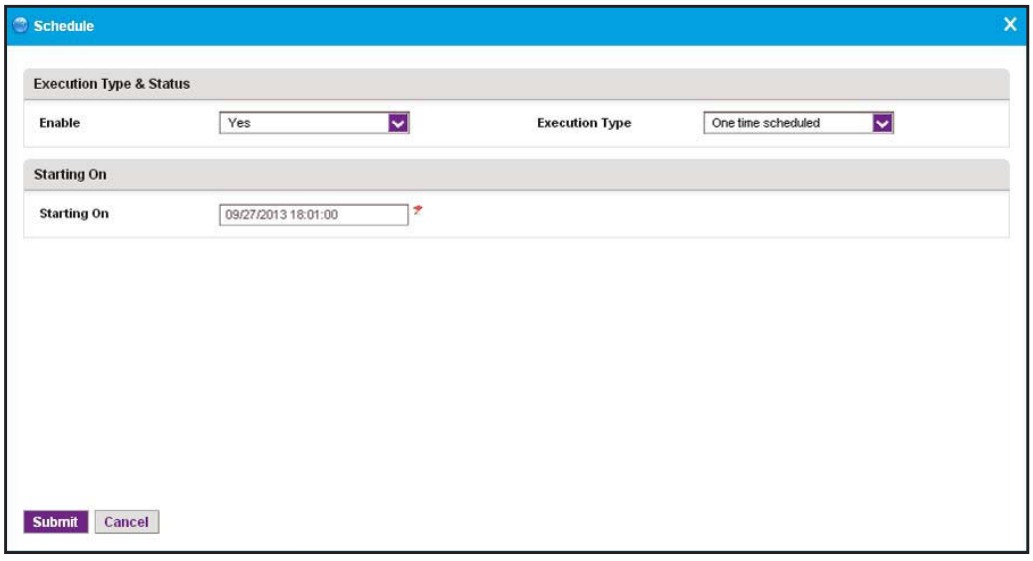


5. Take one of the following actions:
   - To add a new schedule, click the **Add Schedule** button.
   - To modify an existing schedule, click the **Edit Schedule** button.



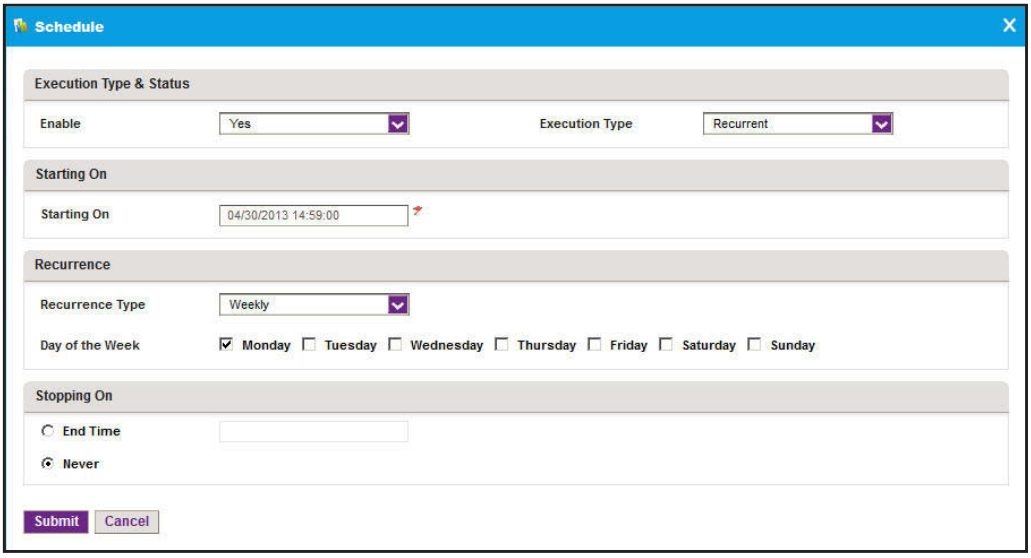
6. From the **Enable** menu, select **Yes**.

   The screen adjusts to display more fields.



7. Specify whether the application executes the discovery job once or on a recurring basis by selecting one of the following options from the **Execution Type** menu and entering or modifying the corresponding information:
   - **One time scheduled**. This is the default selection.

     In the **Starting On** field, enter or modify the date and time.
   - **Recurrent**. The screen adjusts to display more fields.



Enter or modify the following information:

a. In the **Starting On** field, enter or modify the date and time.

b. From the **Recurrence Type** menu, select how the schedule recurs and complete the corresponding field or select the corresponding check boxes.

c. Select the **End Time** radio button and enter or modify the date and time in the corresponding field, or leave the **Never** radio button selected, which is the default setting.

8. Click the **Submit** button.

   The Schedule screen closes. The discovery job schedule becomes part of the discovery profile.

9. On the Edit Profile screen, click the **Save** button.

   Your discovery job is executed according to the schedule that you set.

Note: Output files from completed resource discovery jobs are saved for the data retention period. For more information, see *Set the Data Retention Period* on page 214.

Remove a Device Credential

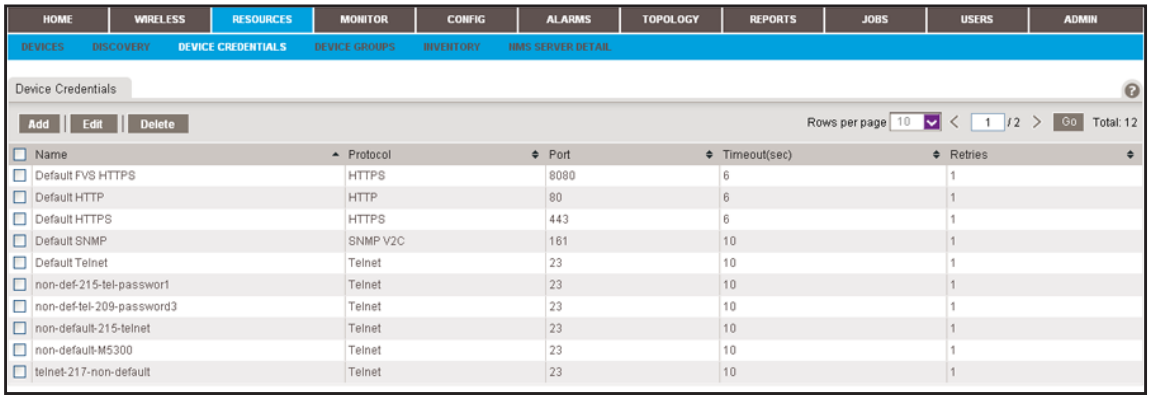
You can remove a device credential that you no longer need.

➢ **To remove a device credential:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICE CREDENTIALS**.



3. Select the device credential.
4. Click the **Delete** button.

   A pop-up confirmation screen displays.

5. Click the **Yes** button.

   The device credential is removed from the Device Credentials table and deleted.

Remove a Discovery Profile

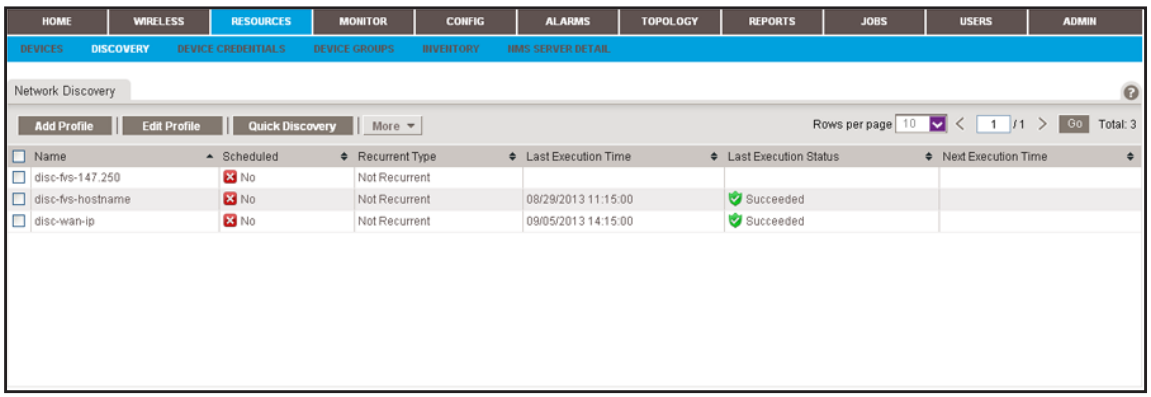
If you delete a discovery job from the Jobs table, the application deletes the discovery profile for the job automatically. For more information, see *View and Manage Jobs* on page 202. You can also remove a discovery profile manually.

➢ **To remove a discovery profile manually:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DISCOVERY**.



3. Select the discovery profile.
4. From the **More** menu, select **Delete**.

A pop-up confirmation screen displays.

5. Click the **Yes** button.

   The discovery profile is removed from the Network Discovery table and deleted.

View and Manage the Wired and Wireless Devices on Your Network

After the application discovers the wired and wireless devices on your network and adds them to the inventory database, you can view and test the devices. The following sections describe the tasks that you can perform:

- *View Device Information*
- *View Wireless Device Information Only*
- *Modify the Name, Location Information, and Contact Information*
- *Remove Device Information*
- *Synchronize a Network Device*
- *Log In to a Device*
- *Ping, Perform a Traceroute, or Reboot a Device*
- *Use the SNMP MIB Browser*
- *View and Export the Inventory Table and Interface List Table*

The application polls the devices to make sure that they are still on the network. You can change how frequently the device inventory is polled. For more information, see *Set the Inventory Polling* on page 215.

View Device Information

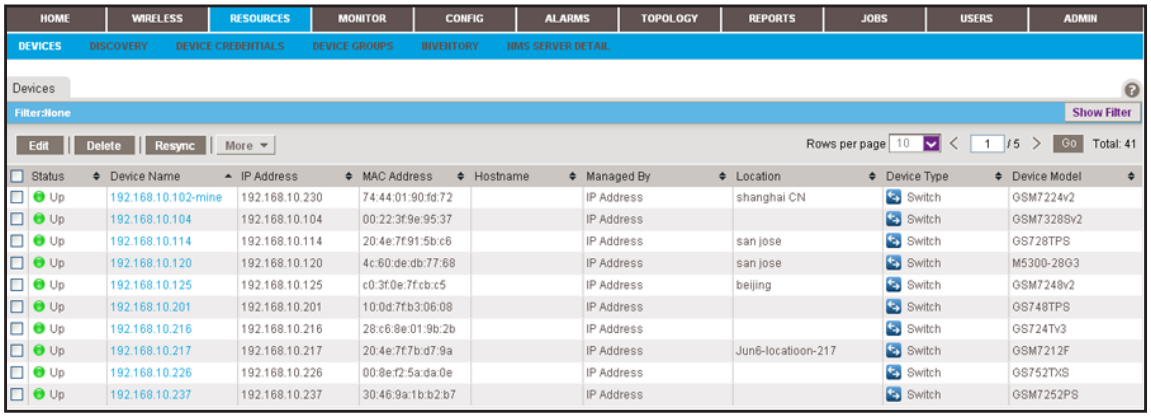
You can see a table of devices that the application discovered in your network.

➢ **To view the Devices table:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICES**.



The screen displays the devices that the application discovered.

3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. To view details about a device, click the device name (or IP address) for the device.

   For more information, see *View Device Details and Interface Details* on page 77.

View Wireless Device Information Only

You can easily monitor your wireless network by displaying wireless controllers, wireless access point (APs), wireless management systems, and active wireless clients.

Note: For information about viewing wireless clients of wireless controllers, APs, and management systems, see *Monitor Wireless Clients and View Client Details* on page 80.

View Wireless Controller Information Only

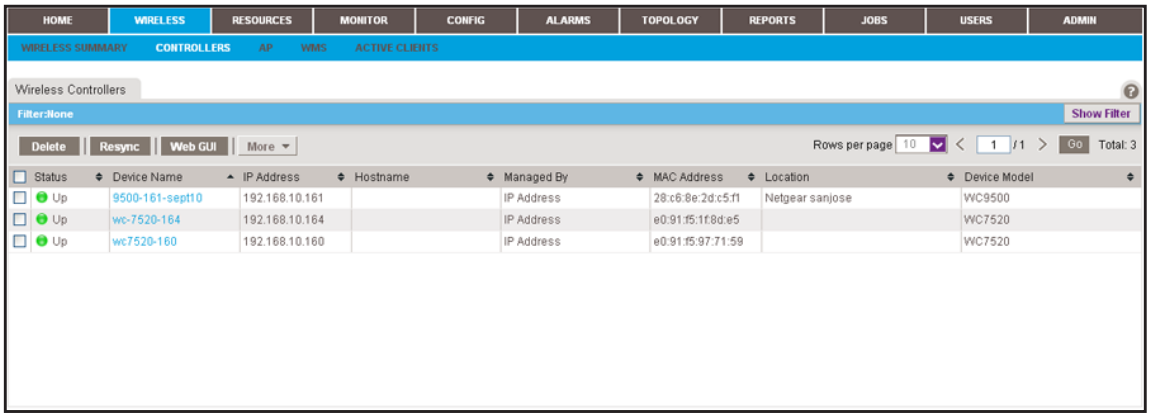
You can display only the wireless controllers that the application manages.

➢ **To view wireless controller information:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **WIRELESS > CONTROLLERS**.



3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, IP Address, Hostname, Managed By, MAC Address, Location, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, and Discover Time.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. To view details about a device, click the device name (or IP address) for the device.

   For more information, see *View Device Details and Interface Details* on page 77.

View Wireless Access Point Information Only

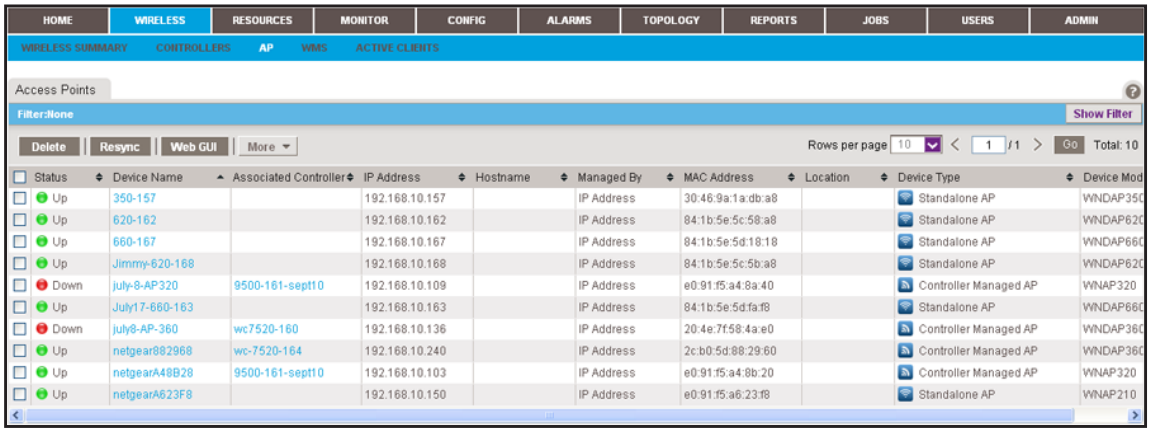
You can display only the standalone APs and controller-managed APs. The application manages the standalone APs. The controller-managed APs are managed by their wireless controllers and display for information only.

➢ **To view wireless access point information:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **WIRELESS > AP**.



3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. To view details about a device, click the device name (or IP address) for the device.

   For more information, see *View Device Details and Interface Details* on page 77.

View Wireless Management System Information Only

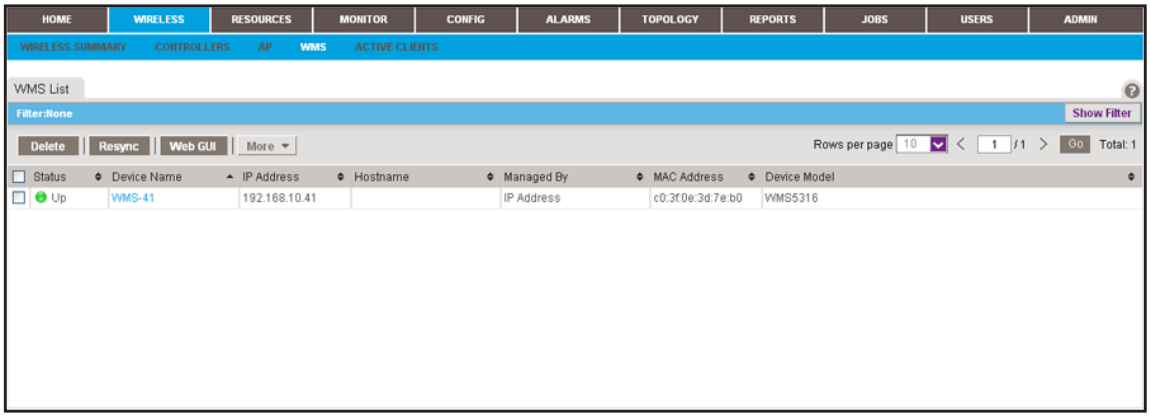
You can display only the wireless management systems that the application manages.

➢ **To view wireless management system information:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **WIRELESS > WMS**.



3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, IP Address, Hostname, Managed By, MAC Address, Device Model, Vendor, Location, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial, Number, Contact, and Discover Time.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. To view details about a device, click the device name (or IP address) for the device.

   For more information, see *View Device Details and Interface Details* on page 77.

Modify the Name, Location Information, and Contact Information

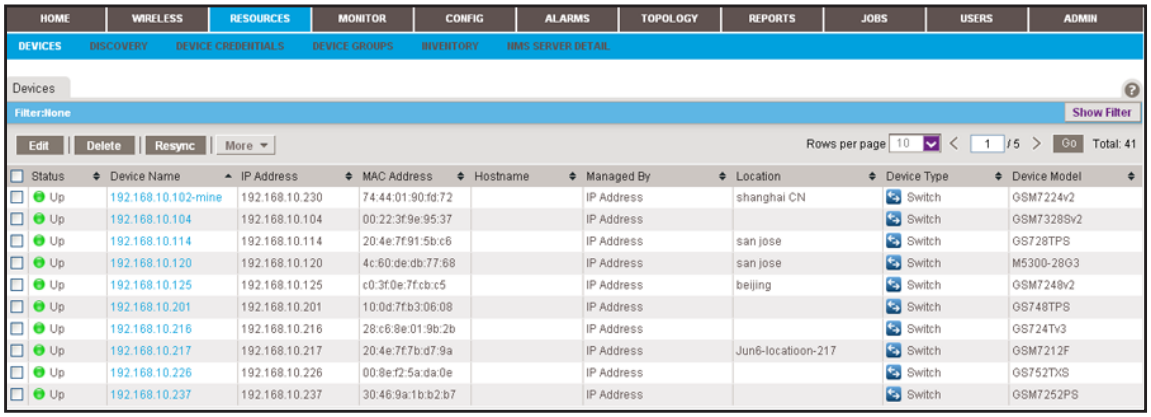
You can modify the device name, location information, and contact information that the application displays for a wired or wireless device.

➢ **To modify information for a device:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICES**.



The screen displays the devices that the application discovered.

3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

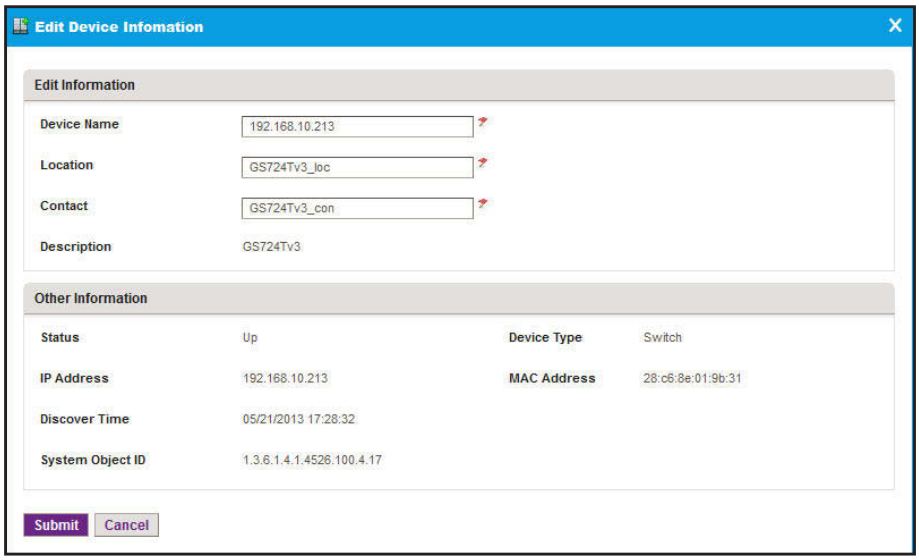
   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. Select the device.
6. Click the **Edit** button.



7. Modify the device information.

8. Click the **Submit** button.

   The device information is updated and the screen closes.

Remove Device Information

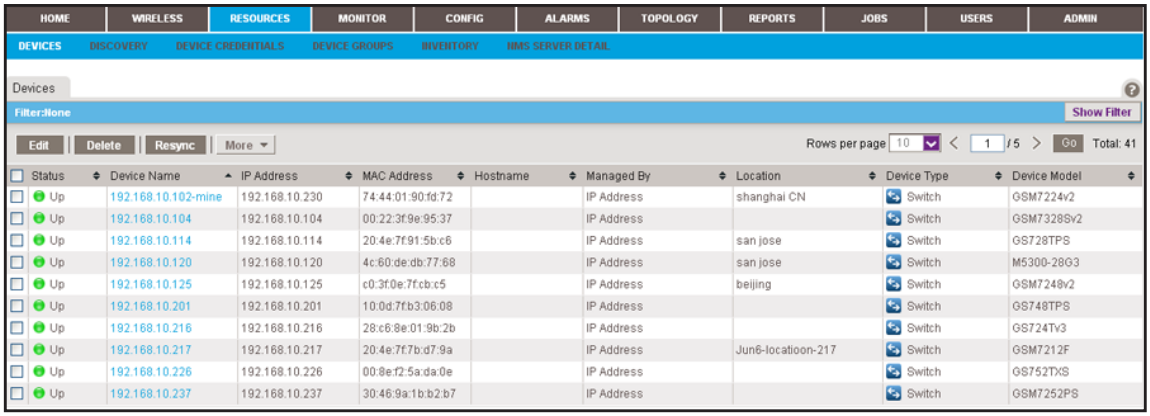
You can remove all information that the application displays for a wired or wireless device. However, when you run another discovery job, the application might rediscover the device and add it again to its inventory database.

➢ **To remove information for a device:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICES**.



   The screen displays the devices that the application discovered.

3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. Select the device.
6. Click the **Delete** button.

   A pop-up confirmation screen displays.

7. Click the **Yes** button.

   The device is removed from the Devices table and deleted.

Synchronize a Network Device

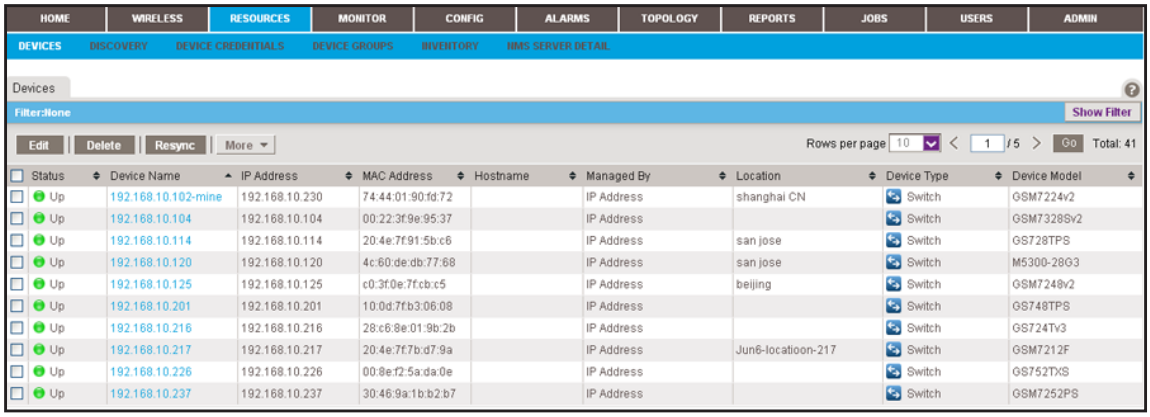
You can time-synchronize a wired or wireless network device to the NMS300 server.

➢ **To synchronize a device:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICES**.



   The screen displays the devices that the application discovered.

3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. Select the device.
6. Click the **Resync** button.

   A pop-up confirmation screen displays.

7. Click the **Yes** button.

   The device is synchronized and the confirmation screen closes.

Log In to a Device

You can log in to a wired or wireless device on your network using either the web management interface or Telnet.

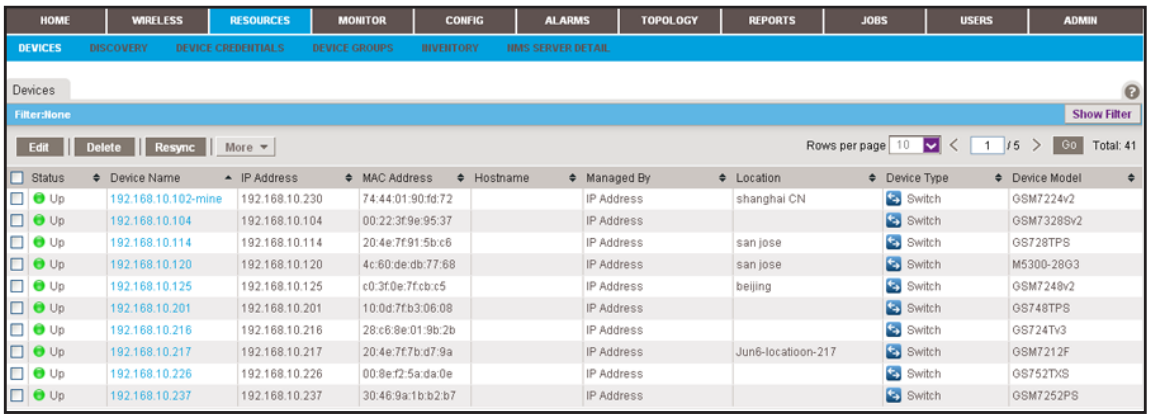
You can log in to a device when your web browser can be routed to the device. Generally, your web browser must be on the local network side of the Internet gateway.

➢ **To log in to a device:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICES**.



   The screen displays the devices that the application discovered.

3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. Select the device.

6. Take one of the following actions:

   - Log in over the web management interface:

     a. From the **More** menu, select **Web GUI**.

     A login screen for the web management interface displays.

     b. Enter the user name and password.

For most NETGEAR products, the user name is **admin** and the password is **password**.

c. Click the button that lets you log in to the device.

The name of the button depends on the device. For most NETGEAR products, the button is called the **Login** button.

- Log in over a Telnet connection:

a. From the **More** menu, select **Telnet**.

A login screen for the CLI displays.

b. Enter the user name and password.

For most NETGEAR products, the user name is **admin** and the password is **password**.

Ping, Perform a Traceroute, or Reboot a Device

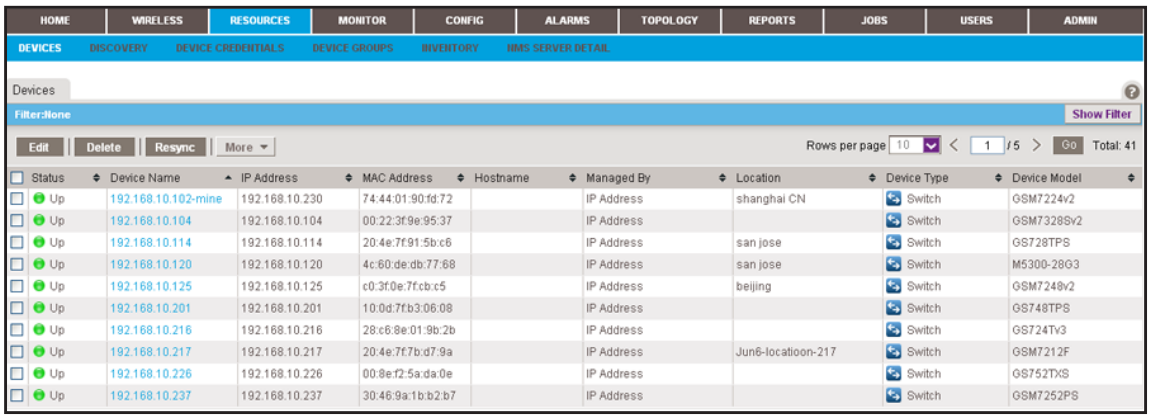
You can ping, perform a traceroute, or reboot a wired or wireless network device from the LAN or WAN. Your web browser must be routed to the NMS300 server to conduct these tasks.

➢ **To test or reboot a device:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICES**.



The screen displays the devices that the application discovered.

3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. Select the device.
6. Take one of the following actions:
   - Ping the device. From the **More** menu, select **Ping**.

     When the ping completes, a screen displays the results.
   - Trace a route. From the **More** menu, select **TraceRoute**.

     When the traceroute completed, a screen displays the results.
   - Reboot the device. From the **More** menu, select **Reboot**.

     Even though you reboot the device, the device remains in the inventory of the application.

Use the SNMP MIB Browser

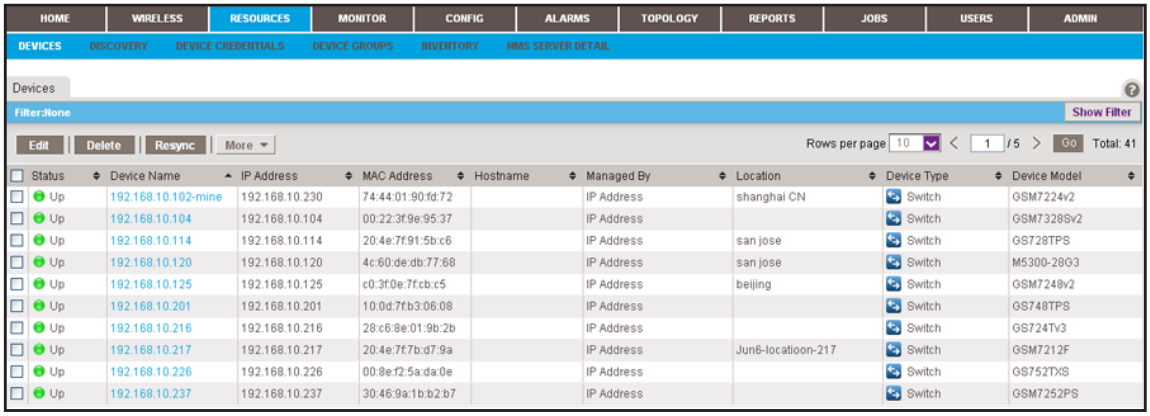
The SNMP MIB browser lets you retrieve information about SNMP-enabled devices directly. The application supports SNMPv1, SNMPv2c, and SNMPv3 and all supported standard and private MIBs. The SNMP MIB browser lets you select one of several MIB databases and navigate a MIB tree to select a specific MIB trap. The application displays the data that the MIB trap collects, information about the selected MIB trap, and information about the SNMP credentials.

➢ **To select a MIB database and a MIB trap, collect data for a device, and view information about the MIB trap and SNMP credentials:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICES**.



   The screen displays the devices that the application discovered.

3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

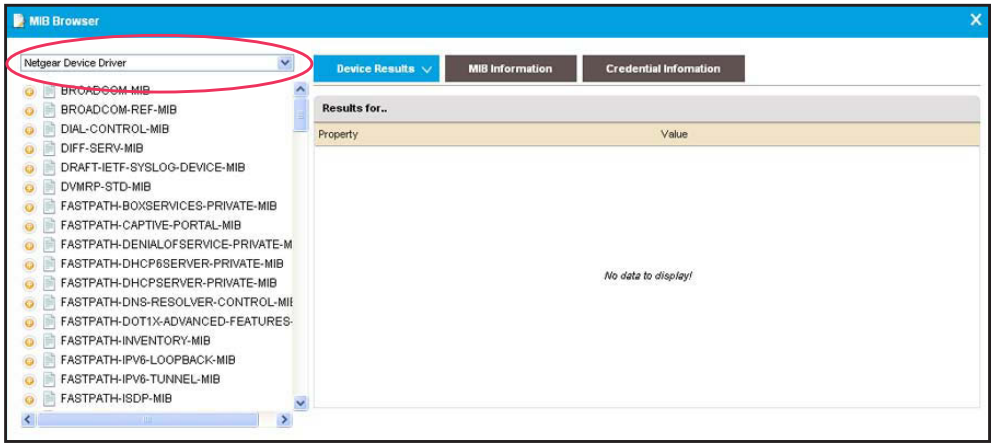
   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

   To hide the filter, click the **Hide Filter** button.

5. Select the device.
6. From the **More** menu, select **MIB Browser**.

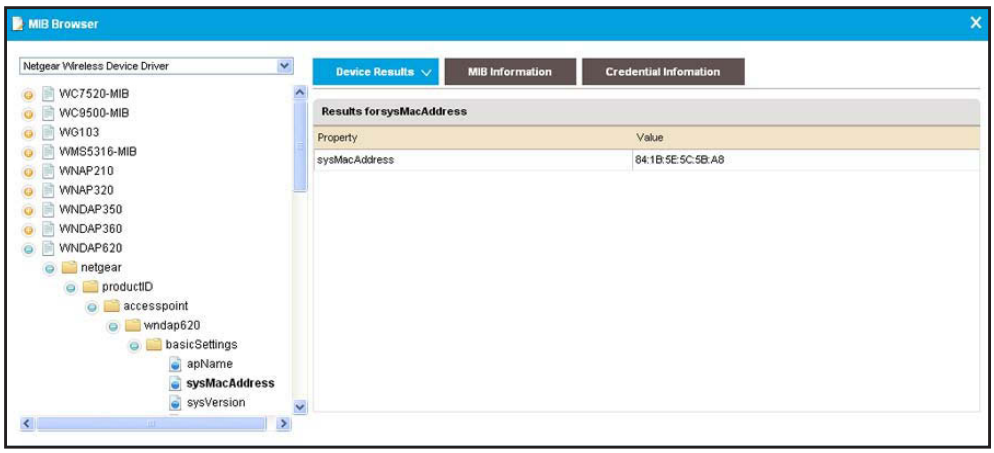


7. From the menu in the upper left of the screen, select the MIB database.

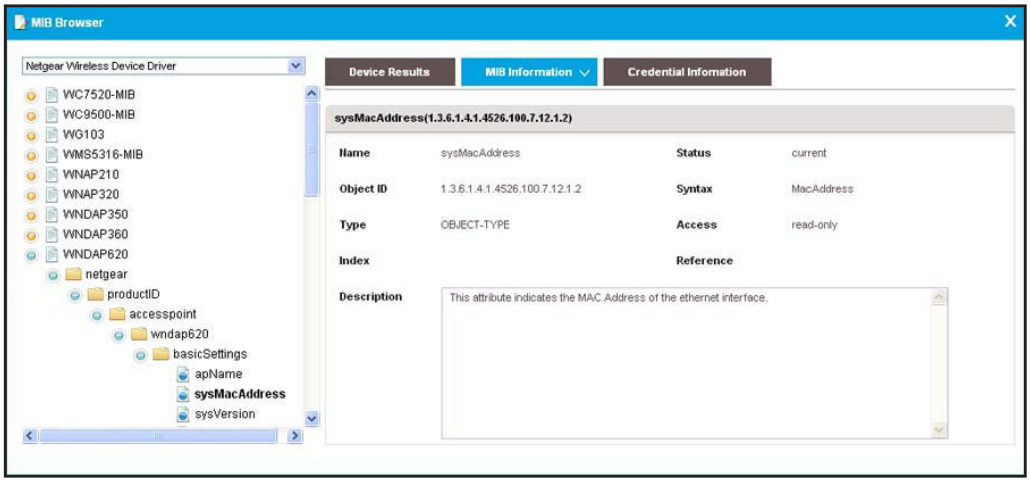
   A MIB tree populates the screen.

8. Navigate to the MIB trap and click the MIB trap.

   The Device Results section of the screen displays the property and value that the MIB trap collects:

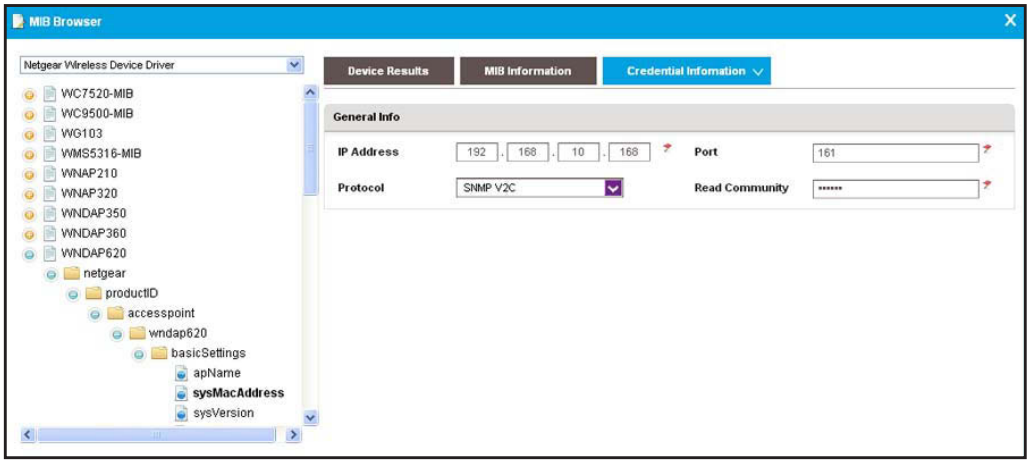


9. To view information about the selected MIB or MIB trap, click the **MIB Information** tab.



The screen displays the name and object ID of the selected MIB or MIB trap, along with a description and other information.

10. To view information about the SNMP credentials for the selected device, click the **Credential Information** tab.



The screen displays the IP address and SNMP port for the device, along with SNMP protocol and read community or SNMP user information.

11. To display the information for another SNMP protocol, select another protocol from the **Protocol** menu.

    The information onscreen adjusts.

12. To close the MIB browser, click the **X** (X) in the upper right of the screen.

View and Export the Inventory Table and Interface List Table

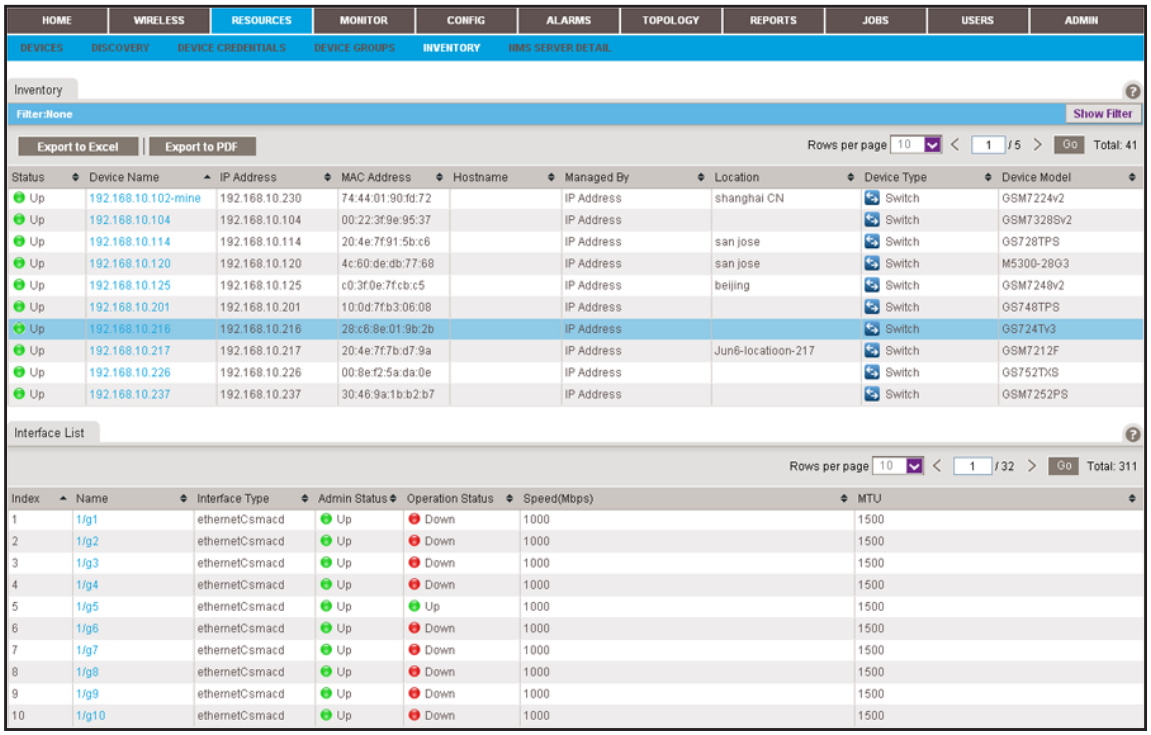
You can view the table of wired and wireless devices and interfaces that the application manages, and export this table to an Excel or PDF file.

➢ **To view and export the Inventory table and Interface List table:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > INVENTORY**.



3. To add columns to or remove them from the Inventory table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, IP Address, MAC Address, Hostname, Managed By, Location, Device Type, Device Model, Vendor, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as device type, device name and IP address, location, device model, and status.

   To hide the filter, click the **Hide Filter** button.

5. To view interfaces for a specific device, click the table row for the device anywhere but in the Device Name column.

6. To view details about an individual device or interface, in the Device Name column, click the device name (or IP address), or, in the Name column, click the interface name.

   For information about viewing device details, see *View Device Details and Interface Details* on page 77.

7. Click the **Export to Excel** button or the **Export to PDF** button.
8. To save the device information on your computer, follow the directions of your browser.

Manage Device Groups

To simplify the management of networks with many devices, you can create device groups. Once they are discovered, you can group the devices on your network by location, device type, and other criteria.

You can create static and dynamic device groups:

- **Static device group**. A fixed group of specific devices that you add manually. For more information, see *Add or Modify a Static Device Group* on page 53.
- **Dynamic device group**. A dynamic list of devices that are selected automatically based on your filter selection criteria. For more information, see *Add or Modify a Dynamic Device Group* on page 55.

For general information about device groups, see *Device Groups* on page 9.

Add or Modify a Static Device Group

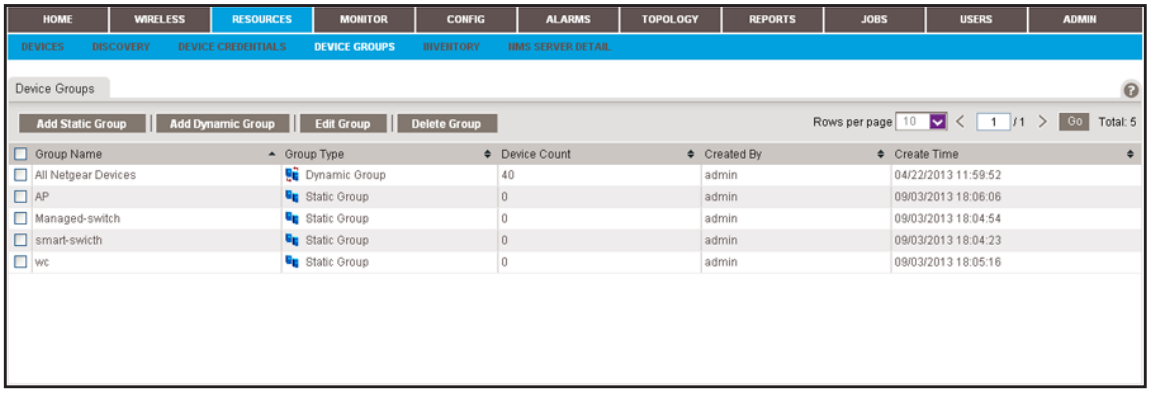
A static group is a fixed list of specific devices. You must add devices manually.

➢ **To add a static device group or modify an existing static device group:**

1. Log in to the application.

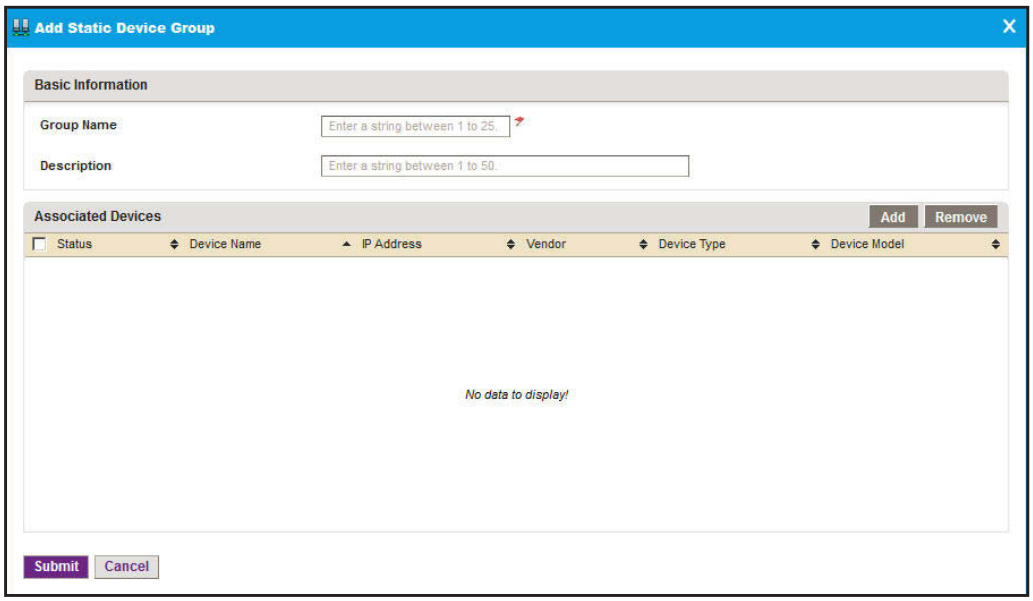
   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICE GROUPS**.

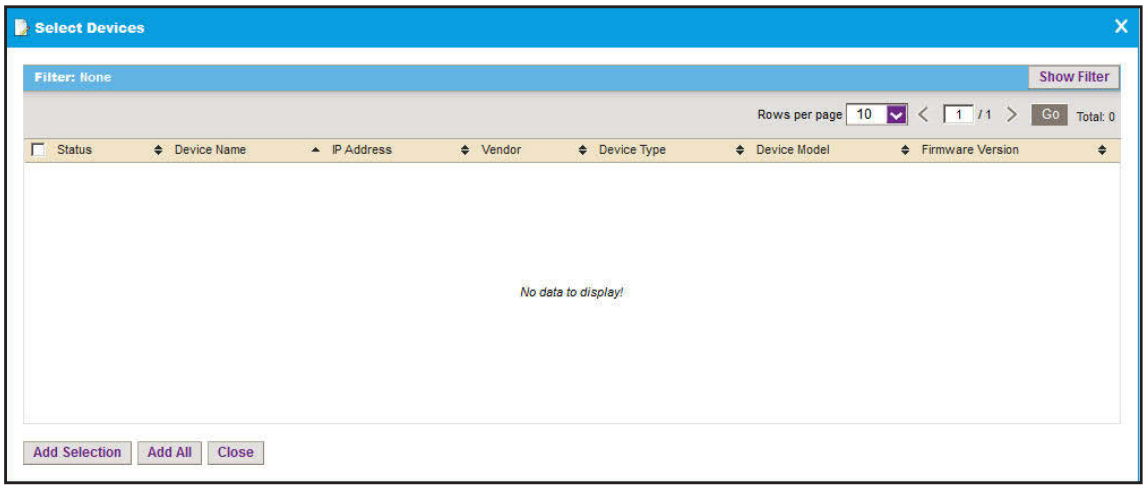


3. Add a static device group or modify an existing static device group:
   - To add a static device group, click the **Add Static Group** button.
   - To modify an existing static device group:
     a. From the Device Groups table, select the static device group.
     b. Click the **Edit Group** button.

   For a new static device group, the Add Static Device Group screen displays. For an existing static device group, the Edit Static Device Group screen displays.



4. Enter or modify the group name.
5. Enter or modify the description.
6. Click the **Add** button.



7. To filter the devices that display on the screen, click the **Show Filter** button.

You can filter the devices by criteria such as device type, device name and IP address, location, device model, and status.

To hide the device filter, click the **Hide Filter** button.

8. On the Select Devices screen, select devices for the group.
9. Click the **Add Selection** button.

   To add all devices, click the **Add All** button.

10. If you are modifying an existing static device group, to remove devices:
    a. Select the devices.
    b. Click the **Remove** button.

    The devices are removed from the Associated Devices table.

11. Click the **Submit** button.

    The screen closes. The devices are added to the static device group, and the group is displayed in the Device Groups table.

Add or Modify a Dynamic Device Group

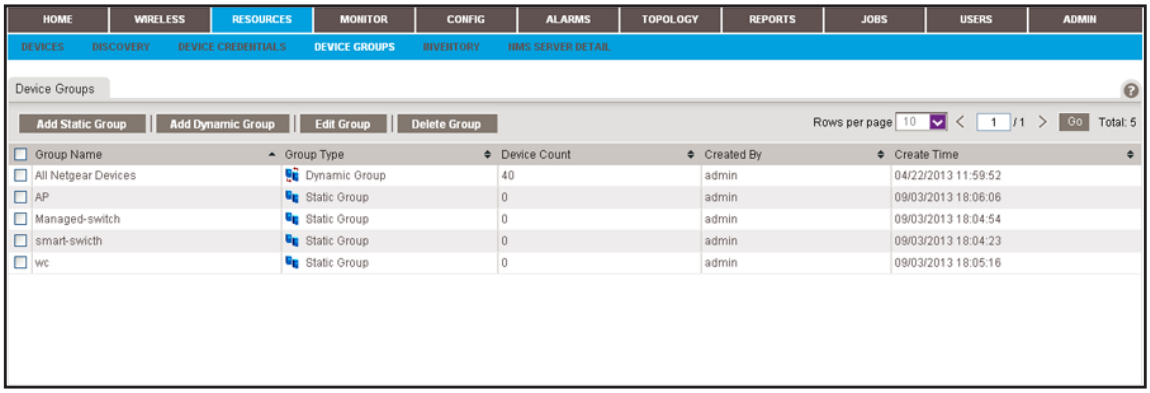
A dynamic group is a dynamic list of devices that are selected automatically based on your filter selection criteria. The list changes automatically as devices that meet the filter criteria are added to and removed from the network.

➢ **To add a dynamic device group or modify an existing dynamic device group:**

1. Log in to the application.

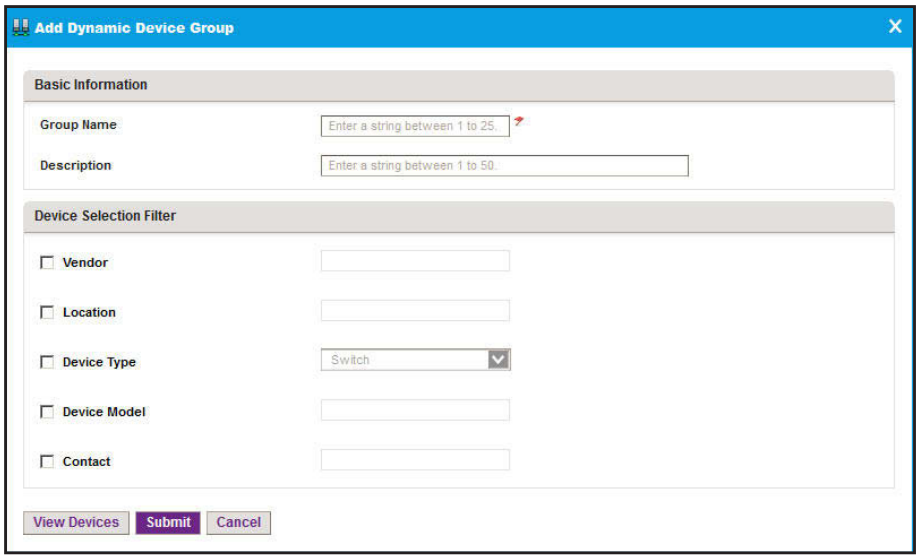
   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICE GROUPS**.



3. Add a dynamic device group or modify an existing dynamic device group:
   - To add a dynamic device group, click the **Add Dynamic Group** button.
   - To modify an existing dynamic device group:
     a. From the Device Groups table, select the dynamic device group.
     b. Click the **Edit Group** button.

For a new dynamic device group, the Add Dynamic Device Group screen displays. For an existing dynamic device group, the Edit Dynamic Device Group screen displays.



4. Enter or modify the group name.
5. Enter or modify the description.
6. Enter or modify the criteria for the device selection filter.

   You can filter by device vendor, device location, device type, device model, and device contact. You can select more than one filter. To filter by device type, make a selection from the **Device Type** menu.
7. To view the devices in the group before you save the group, select the **View Devices** button.

   The devices that meet the selection criteria are displayed.
8. Click the **Submit** button.

   The screen closes. The devices are added to the dynamic device group, and the group is displayed in the Device Groups table.

Remove a Device Group

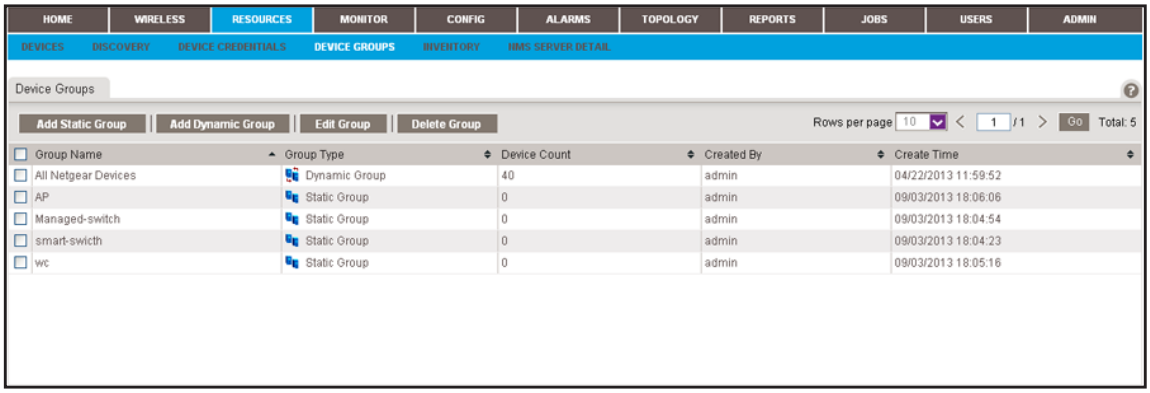
You can remove a device group that you no longer need.

➢ **To remove a device group:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICE GROUPS**.



3. Select the device group.
4. Click the **Delete Group** button.

   A pop-up confirmation screen displays.
5. Click the **Yes** button.

   The device group is removed from the Device Groups table and deleted.

Monitor Devices and the Network

4

Monitor how devices and the network perform

You can view summary and detailed information about the network, devices, and interfaces, including real-time and historical information and performance statistics. You can also enable and disable the configuration monitors, view and export the audit logs, view firmware versions, and view NMS300 server information.

This chapter covers the following topics:

- *Monitor the Network*
- *Monitor the Top 10 Widgets for All Devices*
- *View the Wireless Summary and Monitor the Top 10 Widgets for Wireless Devices*
- *View Device Details and Interface Details*
- *Monitor Wireless Clients and View Client Details*
- *Manage the Configuration Monitors*
- *Customize the Optional Network Dashboard*
- *View and Export Audit Logs*
- *View Firmware Version Information*
- *View the NMS300 Server Information*
- *View Application Notifications*

Monitor the Network

You can monitor the network by various criteria and you can customize the information that displays on the Network Summary screen.

View the Default Network Summary

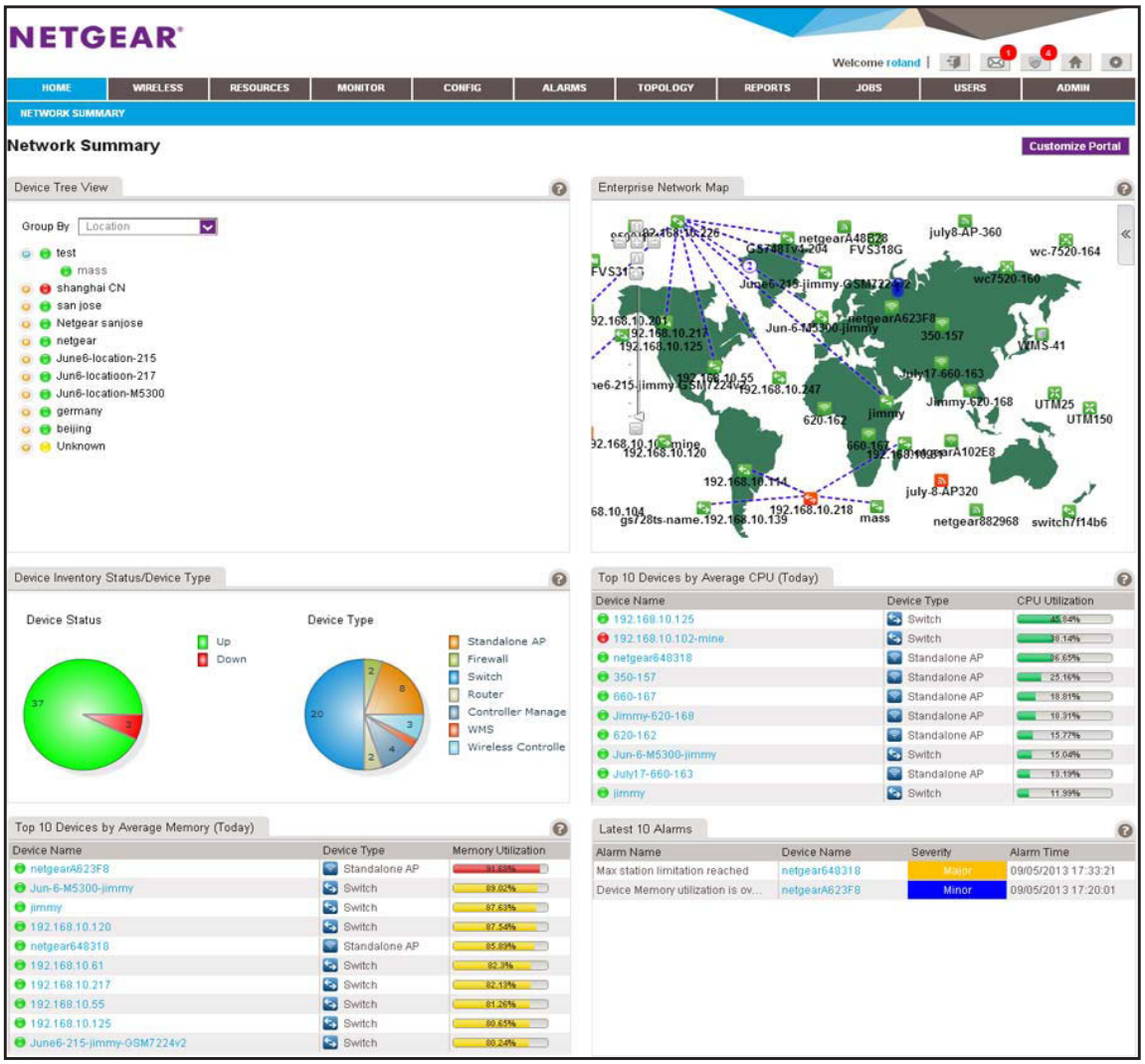
If you have not customized the Network Summary screen, the screen displays a device tree, an enterprise network map, a physical representation of the status and device type of the inventory, and various top 10 widgets.

➢ **To view the default network summary:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **HOME > NETWORK SUMMARY**.



By default, the following widgets display onscreen.

Widget	Description	Information
Device Tree View	A tree of all discovered and managed devices in the network. You can expand the tree.	Group devices by: • Location (the default setting) • Vendor • Device Type • Device Group
Enterprise Network Map	A world map that displays the location of each device and its connections to other devices	• Manual link • LLDP link • < 1.5 Mbps link • >= 1.5 Mbps < 10 Mbps link • >= 10 Mbps < 100 Mbps link • >= 100 Mbps < 1 Gbps link • >= 1 Gbps < 10 Gbps link • >= 10 Gbps link • Link of unknown speed
Device Inventory Status/Device Type	A slice graph displaying the device status (Up or Down) and a slice graph displaying the network breakdown per device type.	
Top 10 Devices by Average CPU (Today)	Top 10 devices by average CPU utilization for today	• Device status • Device name • Device type • CPU utilization in percentage
Top 10 Devices by Average Memory (Today)	Top 10 devices by average memory utilization for today	• Device status • Device name • Device type • Memory utilization in percentage
Latest 10 Alarms		• Alarm Name • Device Name • Severity • Alarm Time

3. To view details about a device, click the device name.

   For more information, see *View Device Details and Interface Details* on page 77.

Customize the Network Summary Screen

You can customize the items that display on the Network Summary screen. You do not need to be an admin user to customize the Network Summary screen.

In addition to the default widgets that are shown in the table in *View the Default Network Summary* on page 59, you can add the optional widgets that are listed in the following table.

Table 1. Optional widgets for the Network Summary screen

Widget	Description	Information
Devices		
Top 10 Devices by Average Response Time (Today)	Top 10 devices by average response time for today	• Device status • Device name • Device type • Average response time in ms
Top 10 Devices by Average Packet Loss (Today)	Top 10 devices by average packet loss percentage for today	• Device status • Device name • Device type • Average packet loss in percentage
Interfaces		
Top 10 Interfaces by Utilization (Today)	Top 10 interfaces by interface utilization for today	• Device status • Device name • Interface status • Interface name • Ingress (Rx) utilization in percentage • Egress (Tx) utilization in percentage • Total utilization in percentage
Top 10 Interfaces by Traffic Rate (Today)	Top 10 interfaces by traffic rate for today	• Device status • Device name • Interface status • Interface name • Ingress (Rx) traffic rate • Egress (Tx) traffic rate • Total traffic rate **Note:** Traffic rate is stated in bps, Kbps, or Mbps.

Table 1. Optional widgets for the Network Summary screen (continued)

Widget	Description	Information
Top 10 Interfaces by Traffic (Today)	Top 10 interfaces by total traffic for today	• Device status • Device name • Interface status • Interface name • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume **Note:** Traffic volume is stated in KB, MB, or GB.
Top 10 Interfaces by Errors (Today)	Top 10 interfaces by total errors for today	• Device status • Device name • Interface status • Interface name • Number of ingress (Rx) errors • Number of egress (Tx) errors • Total number of errors
Top 10 Interfaces by Discards (Today)	Top 10 interfaces by total discarded packets for today	• Device status • Device name • Interface status • Interface name • Number of discarded egress (Tx) packets • Number of discarded ingress (Rx) packets • Total number of discarded packets

➢ **To customize the Network Summary screen:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **HOME > NETWORK SUMMARY**.

   The Network Summary screen displays.

3. Click the **Customize Portal** button.

The screen displays the widgets that are currently selected. The left side of the screen displays the **Available Widgets** menu.

4. Customize the Network Summary screen by performing one of the following tasks:
   - **Add a widget**. From the **Available Widgets** menu, click and drag a widget to an empty widget area at the bottom of the screen. When the widget is in the target widget area, the widget area displays green and you can drop the widget.

     Table 1 on page 61 describes the optional widgets that you can add.
   - **Remove a widget**. In a widget area that is populated by a widget, click the **X** ( ) in the upper right of the widget area.
   - **Adjust the widget order**. To move a widget to another widget area, click and drag the title bar of the widget. When the widget is in the target widget area, the widget area displays green and you can drop the widget.
   - **Remove all widgets**. Click the **Remove All** button.
   - **Reset the Network Summary screen to its defaults**. Click the **Default** button.
5. Repeat *Step 4* until you have selected all widgets that you want to display on the Network Summary screen.
6. If you are not content with your selections, click the **Reset** button and repeat *Step 4* and *Step 5*.
7. Click the **Save** button.

   The settings are saved for your account.
8. (Optional) Select **HOME > NETWORK SUMMARY**.

   The screen displays its customized settings.

Monitor the Top 10 Widgets for All Devices

You can monitor the status and top 10 widgets for devices on the network by various criteria and you can customize the information that displays on the Top 10 screen.

View the Default Top 10 Widgets

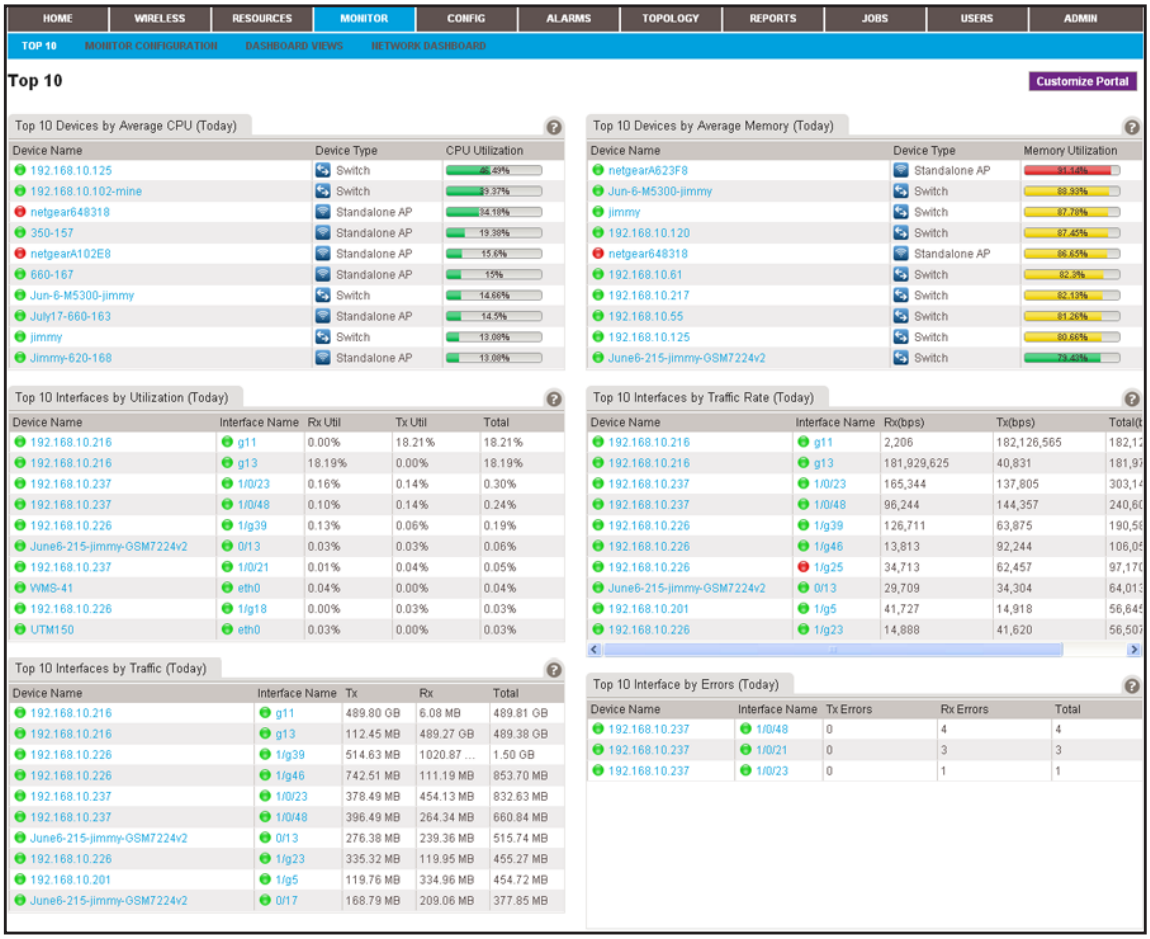
If you have not customized the Top 10 screen, the screen displays the default top 10 widgets.

➢ **To monitor the default top 10 widgets and view device details:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **MONITOR > TOP 10**.



By default, the following widgets display onscreen.

Widget	Description	Information
Top 10 Devices by Average CPU (Today)	Top 10 devices by average CPU utilization for today	• Device status • Device name • Device type • CPU utilization in percentage
Top 10 Devices by Average Memory (Today)	Top 10 devices by average memory utilization for today	• Device status • Device name • Device type • Memory utilization in percentage
Top 10 Interfaces by Utilization (Today)	Top 10 interfaces by interface utilization for today	• Device status • Device name • Interface status • Interface name • Ingress (Rx) utilization in percentage • Egress (Tx) utilization in percentage • Total utilization in percentage

Widget	Description	Information
Top 10 Interfaces by Traffic Rate (Today)	Top 10 interfaces by traffic rate for today	• Device status • Device name • Interface status • Interface name • Ingress (Rx) traffic rate • Egress (Tx) traffic rate • Total traffic rate **Note:** Traffic rate is stated in bps, Kbps, or Mbps.
Top 10 Interfaces by Traffic (Today)	Top 10 interfaces by total traffic for today	• Device status • Device name • Interface status • Interface name • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume **Note:** Traffic volume is stated in KB, MB, or GB.
Top 10 Interfaces by Errors (Today)	Top 10 interfaces by total errors for today	• Device status • Device name • Interface status • Interface name • Number of ingress (Rx) errors • Number of egress (Tx) errors • Total number of errors

3. To view details about a device, click the device name.

   For more information, see *View Device Details and Interface Details* on page 77.

4. To view details about an interface, click the interface name.

   For more information, see *View Device Details and Interface Details* on page 77.

Customize the Top 10 Screen

You can customize the information that displays on the Top 10 screen by adding and removing widgets. You can also reset the screen to its default information.

In addition to the default widgets that are shown in the table in *View the Default Top 10 Widgets* on page 64, you can add the optional widgets that are listed in the following table.

Table 2. Optional widgets for the Top 10 screen

Widget	Description	Information
Top 10 Device		
Top 10 Devices by Average Response Time (Today)	Top 10 devices by average response time for today	• Device status • Device name • Device type • Average response time in ms
Top 10 Devices by Average Packet Loss (Today)	Top 10 devices by average packet loss percentage for today	• Device status • Device name • Device type • Average packet loss in percentage
Top 10 Interface		
Top 10 Interfaces by Discards (Today)	Top 10 interfaces by total discarded packets for today	• Device status • Device name • Interface status • Interface name • Number of discarded egress (Tx) packets • Number of discarded ingress (Rx) packets • Total number of discarded packets
Top 10 Standalone AP		
Top 10 Standalone AP by CPU Utilization (Today)	Top 10 wireless standalone APs by total CPU utilization for today	• Device status • Device name • Device type • CPU utilization in percentage
Top 10 Standalone AP by WLAN Utilization (Today)	Top 10 wireless standalone APs by total WLAN utilization for today	• Device status • Device name • Device type • WLAN utilization in percentage
Top 10 AP by Client Count (Current)	Top 10 wireless standalone APs and controller-managed APs by number of current clients	• Device status • Device name • Device type • Total number of clients
Top 10 Standalone AP by Wired traffic (Today)	Top 10 wireless standalone APs by traffic volume over a wired connection for today	• Device status • Device name • Device type • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume **Note:** Traffic volume is stated in KB, MB, or GB.

Table 2. Optional widgets for the Top 10 screen (continued)

Widget	Description	Information
Top 10 SSID		
Top 10 SSID by Client Count (Current)	Top 10 SSIDs by number of current clients	• SSID • Device status • Device name • Radio • Total number of clients
Top 10 SSID by Traffic (Today)	Top 10 SSIDs by traffic volume for today	• SSID • Device status • Device name • Radio • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume **Note:** Traffic volume is stated in KB, MB, or GB.
Top 10 Radio		
Top 10 Radio by Client Count (Current)	Top 10 radios by number of current clients	• Radio • Device status • Device name • Device type • Total number of clients
Top 10 Radio by Traffic (Today)	Top 10 radios by traffic volume for today	• Radio • Device status • Device name • Device type • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume **Note:** Traffic volume is stated in KB, MB, or GB.

➢ **To customize the Top 10 screen:**

1. Log in to the application.

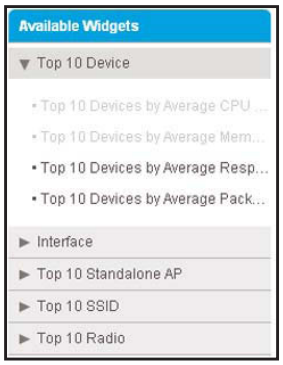
   For more information, see *Log In to the Application* on page 15.

2. Select **MONITOR > TOP 10**.

   The Top 10 screen displays.

3. Click the **Customize Portal** button.

The screen displays the widgets that are currently selected. The left side of the screen displays the **Available Widgets** menu.


Available Widgets
Top 10 Device
Top 10 Devices by Average CPU ...
Top 10 Devices by Average Mem...
Top 10 Devices by Average Resp...
Top 10 Devices by Average Pack...
Interface
Top 10 Standalone AP
Top 10 SSID
Top 10 Radio

4. Customize the Top 10 screen by performing one of the following tasks:
   - **Add a widget**. From the **Available Widgets** menu, click and drag a widget to an empty widget area at the bottom of the screen. When the widget is in the target widget area, the widget area displays green and you can drop the widget.

     Table 2 on page 67 describes the optional widgets that you can add.
   - **Remove a widget**. In a widget area that is populated by a widget, click the **X** (X) in the upper right of the widget area.
   - **Adjust the widget order**. To move a widget to another widget area, click and drag the title bar of the widget. When the widget is in the target widget area, the widget area displays green and you can drop the widget.
   - **Remove all widgets**. Click the **Remove All** button.
   - **Reset the Top 10 screen to its defaults**. Click the **Default** button.
5. Repeat *Step 4* until you have selected all widgets that you want to display on the Top 10 screen.
6. If you are not content with your selections, click the **Reset** button and repeat *Step 4* and *Step 5*.
7. Click the **Save** button.

   Your changes are saved.
8. (Optional) Select **MONITOR > TOP 10**.

   The screen displays its customized settings.

View the Wireless Summary and Monitor the Top 10 Widgets for Wireless Devices

You can monitor the wireless inventory and top 10 widgets for wireless devices on the network by various criteria and you can customize the information that displays on the Wireless Summary screen.

View the Wireless Summary and Default Top 10 Wireless Widgets

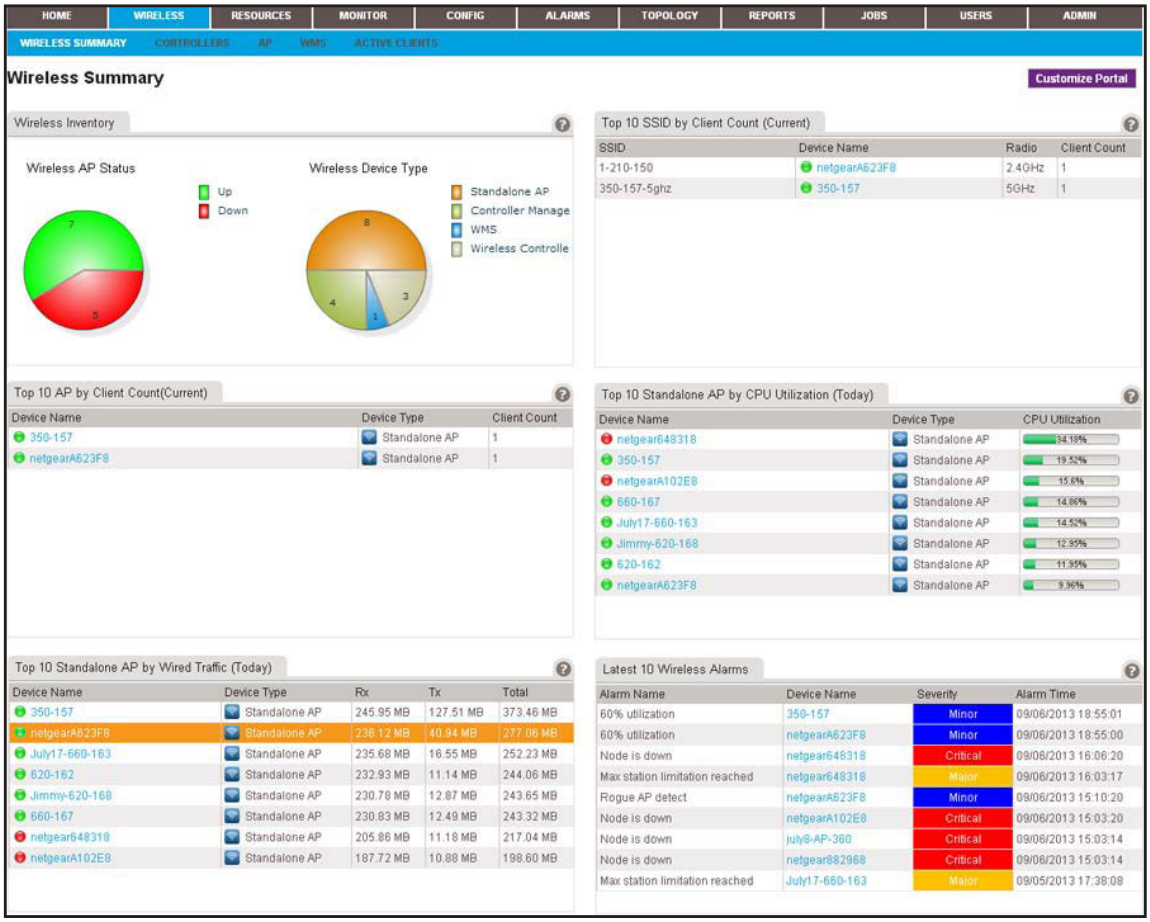
If you have not customized the Wireless Summary screen, the screen displays the wireless inventory and default top 10 widgets for wireless devices.

- **To monitor the wireless inventory, monitor the default top 10 widgets for wireless devices, and view wireless device details:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **WIRELESS > WIRELESS SUMMARY**.



By default, the following widgets display onscreen.

Widget	Description	Information
Wireless Inventory	Status of the wireless APs and distribution of wireless devices in the network	• Wireless AP status: - Number of APs that are up - Number of APs that are down • Wireless device type: - Number of standalone APs - Number of controller-managed APs - Number of wireless management systems (WMSs) - Number of wireless controllers
Top 10 SSID by Client Count (Current)	Top 10 SSIDs by number of current clients	• SSID • Device status • Device name • Radio • Total number of clients
Top 10 AP by Client Count (Current)	Top 10 wireless standalone APs and controller-managed APs by number of current clients	• Device status • Device name • Device type • Total number of clients
Top 10 Standalone AP by CPU Utilization (Today)	Top 10 wireless standalone APs by total CPU utilization for today	• Device status • Device name • Device type • CPU utilization in percentage
Top 10 Standalone AP by Wired traffic (Today)	Top 10 wireless standalone APs by traffic volume over a wired connection for today	• Device status • Device name • Device type • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume **Note:** Traffic volume is stated in KB, MB, or GB.
Latest 10 Wireless Alarms		• Alarm name • Device name • Severity • Alarm time

3. To view details about a device, click the device name.

   For more information, see *View Device Details and Interface Details* on page 77.

Customize the Wireless Summary Screen

You can customize the information that displays on the Wireless Summary screen by adding and removing widgets. You can also reset the screen to its default information.

In addition to the default widgets that are shown in the table in *View the Wireless Summary and Default Top 10 Wireless Widgets* on page 71, you can add the optional widgets that are listed in the following table.

Table 3. Optional widgets for Wireless Summary screen

Widget	Description	Information
Top 10 Standalone AP		
Top 10 Standalone AP by Memory Utilization (Today)	Top 10 wireless standalone APs by total memory utilization for today	• Device status • Device name • Device type • Memory utilization in percentage
Top 10 Standalone AP by WLAN Utilization (Today)	Top 10 wireless standalone APs by total WLAN utilization for today	• Device status • Device name • Device type • WLAN utilization in percentage
Top 10 SSID		
Top 10 SSID by Traffic (Today)	Top 10 SSIDs by traffic volume for today	• SSID • Device status • Device name • Radio • Egress (Tx) traffic volume • Ingress (Rx) traffic volume • Total traffic volume **Note:** Traffic volume is stated in KB, MB, or GB.

Table 3. Optional widgets for Wireless Summary screen (continued)

Widget	Description	Information
Top 10 Radio		
Top 10 Radio by Client Count (Current)	Top 10 radios by number of current clients	• Radio • Device status • Device name • Device type • Total number of clients
Top 10 Radio by Traffic (Today)	Top 10 radios by traffic volume for today	• Radio • Device status • Device name • Device type • Ingress (Rx) traffic volume • Egress (Tx) traffic volume • Total traffic volume **Note:** Traffic volume is stated in KB, MB, or GB.

➢ **To customize the Wireless Summary screen:**

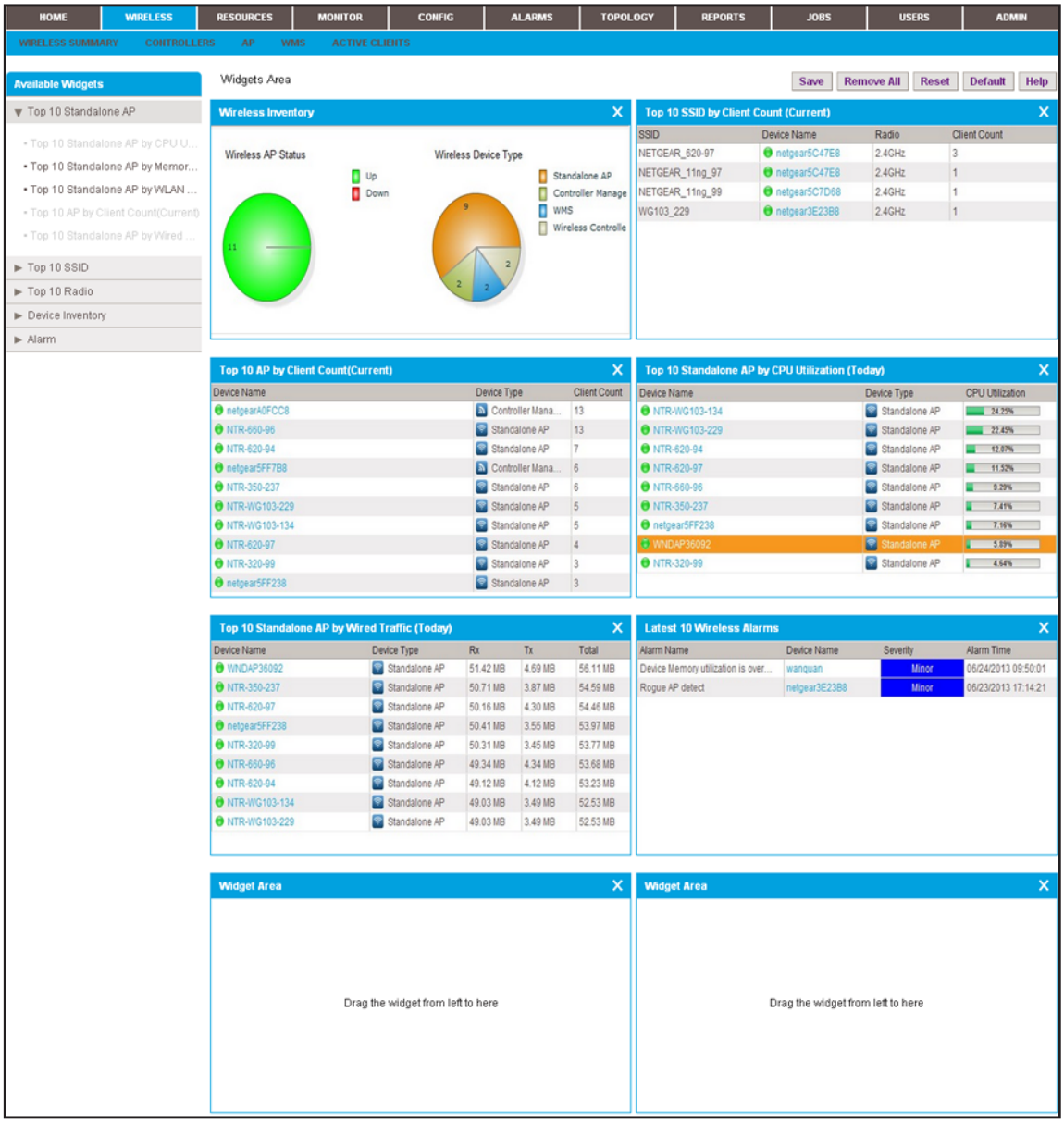
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

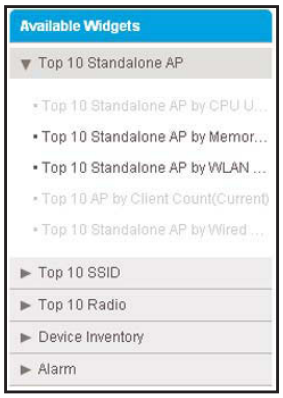
2. Select **WIRELESS > WIRELESS SUMMARY**.

   The Wireless Summary screen displays.

3. Click the **Customize Portal** button.



The screen displays the widgets that are currently selected. The left side of the screen displays the **Available Widgets** menu.


Available Widgets
Top 10 Standalone AP
Top 10 Standalone AP by CPU U...
Top 10 Standalone AP by Memor...
Top 10 Standalone AP by WLAN ...
Top 10 AP by Client Count(Current)
Top 10 Standalone AP by Wired ...
Top 10 SSID
Top 10 Radio
Device Inventory
Alarm

4. Customize the Wireless Summary screen by performing one of the following tasks:
   - **Add a widget**. From the **Available Widgets** menu, click and drag a widget to an empty widget area at the bottom of the screen. When the widget is in the target widget area, the widget area displays green and you can drop the widget.

     Table 3 on page 73 describes the optional widgets that you can add.
   - **Remove a widget**. In a widget area that is populated by a widget, click the **X** (X) in the upper right of the widget area.
   - **Adjust the widget order**. To move a widget to another widget area, click and drag the title bar of the widget. When the widget is in the target widget area, the widget area displays green and you can drop the widget.
   - **Remove all widgets**. Click the **Remove All** button.
   - **Reset the Wireless Summary screen to its defaults**. Click the **Default** button.
5. Repeat *Step 4* until you have selected all widgets that you want to display on the Wireless Summary screen.
6. If you are not content with your selections, click the **Reset** button and repeat *Step 4* and *Step 5*.
7. Click the **Save** button.

   Your changes are saved.
8. (Optional) Select **WIRELESS > WIRELESS SUMMARY**.

   The screen displays its customized settings.

View Device Details and Interface Details

You can view many details for a device and its interfaces. The detailed information that the application can provide depends on the type of device. The Devices table can list the following devices in the Device Type column:

- Switch
- Firewall
- Standalone AP
- Controller-Managed AP
- Wireless Controller
- WMS
- Router
- Unknown

For information about the details that the application can provide for each type of device, see *Appendix B, Device Details*.

For information about NETGEAR products that the application supports, see *Compatible Devices* on page 10.

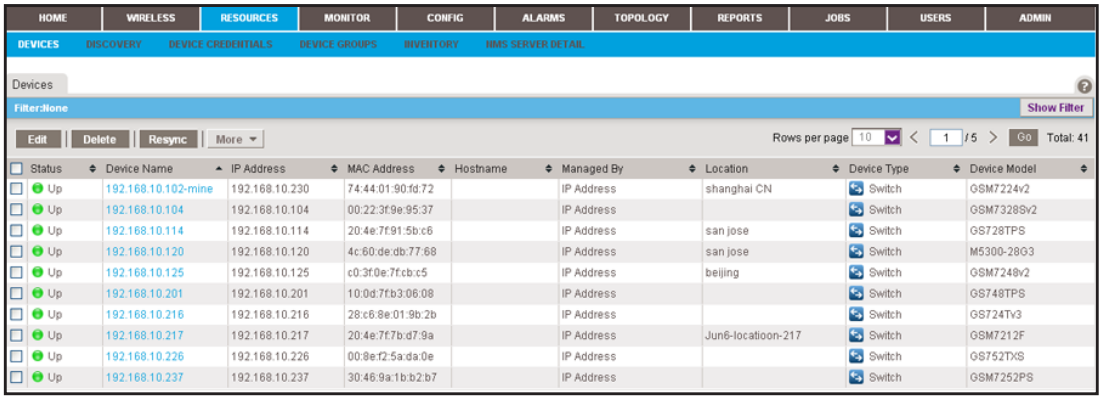
➢ **To view the detailed information for a device and an interface:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > DEVICES**.

   The Devices screen displays.



   The screen displays the devices that the application discovered.

3. To add columns to or remove them from the Devices table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, Device Name, Associated Controller, IP Address, Hostname, Managed By, MAC Address, Location, Device Type, Device Model, Vendor, Device Type, Last Update Time, Hardware Version, Firmware Version, Configuration Version, Serial Number, Contact, Discover Time, and Description.

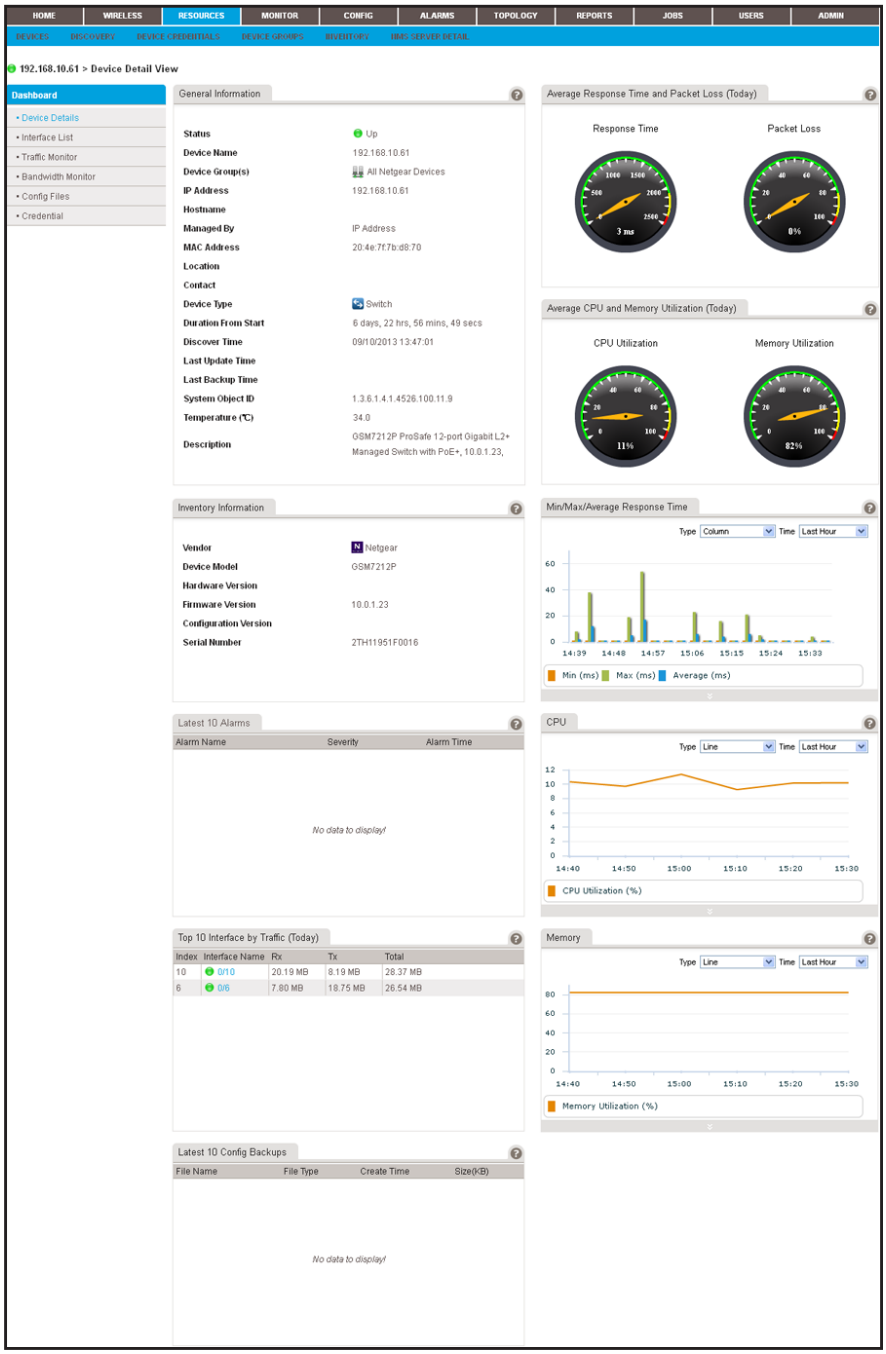
4. To filter the devices that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as type, name, IP address, location, vendor, model, and status.

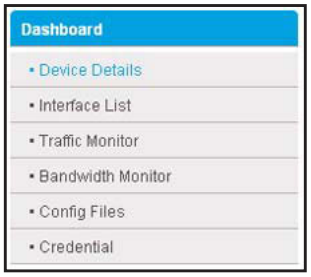
   To hide the filter, click the **Hide Filter** button.

5. Click the name of the device.

   The following figure shows the screen that displays when the device that you select is a switch.



The following figure shows the **Dashboard** menu that displays when the device that you select is a switch.



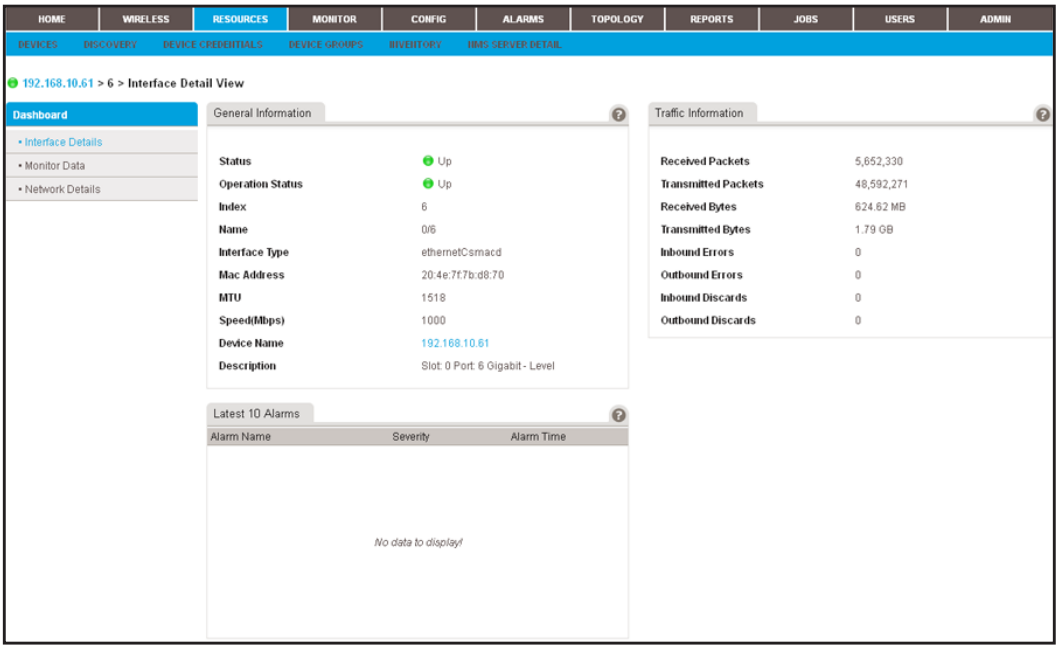
6. From the **Dashboard** menu, select a menu option.

   The screen adjusts to display information that corresponds to your menu option. For information about the details that the application can provide for each type of device, see *Appendix B, Device Details*.

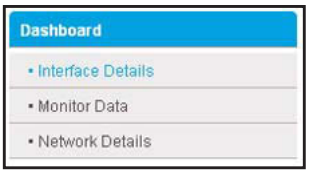
   For switches, wireless controllers, wireless management systems, and routers, you can display interface details.

7. To display interface details:

   a. Select **Interface List**.



   The following figure shows the **Dashboard** menu for an interface:



   b. From the **Dashboard** menu, select a menu option.

The screen adjusts to display information that corresponds to your menu option.

For more information about the details that the application can provide for an interface, see *Appendix B, Device Details*.

Monitor Wireless Clients and View Client Details

The application lets you monitor the active wireless clients by wireless controller, standalone AP, controller-managed AP, or SSID.

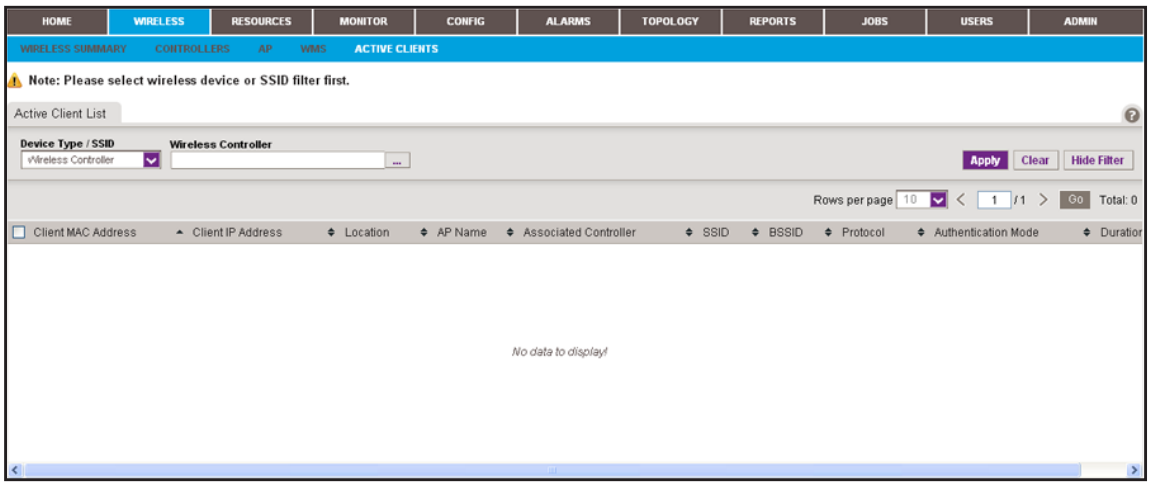
You can display various wireless details for each client.

➢ **To monitor wireless clients and view details for a single client:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **WIRELESS > ACTIVE CLIENTS**.



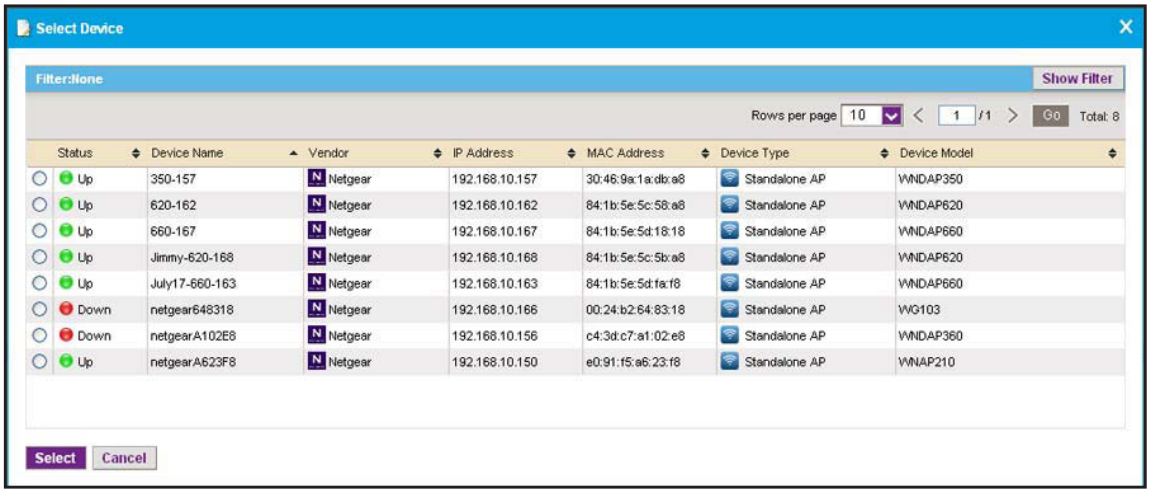
   By default, the filter for active clients is active because the Active Client List table can display many wireless clients.

3. To hide the filter for active clients, click the **Hide Filter** button and go to *Step 10*.
4. From the **Device Type / SSID** menu, select **Wireless Controller**, **Standalone AP**, **Controller Managed AP**, or **SSID**.

   The name of the field to the right of the **Device Type / SSID** menu adjusts according to your selection from the menu.

5. Click the dots next to the field to the right of the **Device Type / SSID** menu.

A screen similar to the following displays.

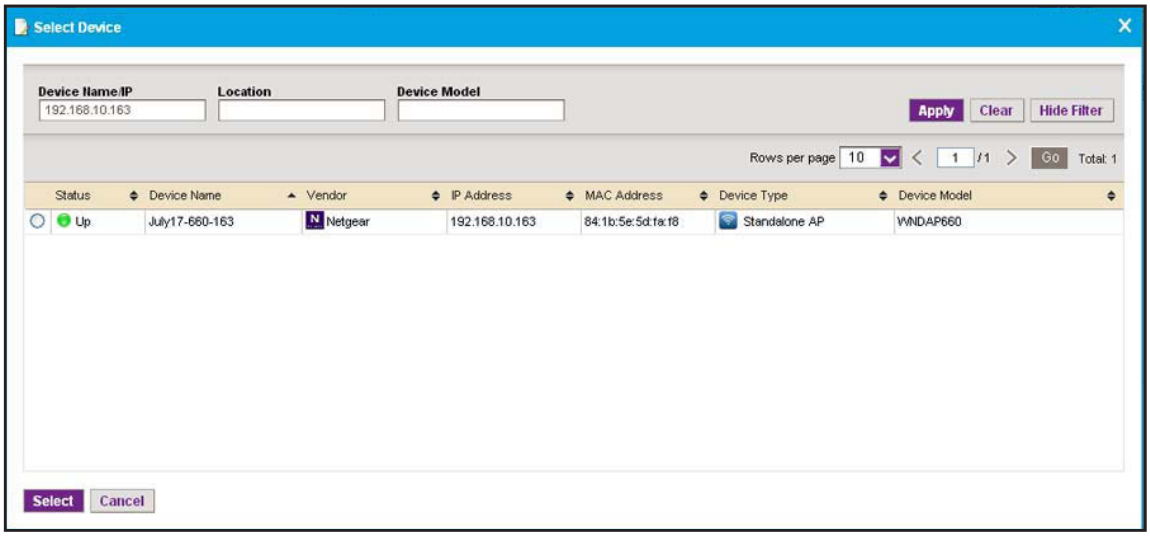

Select Device
Filter:None
Show Filter
Rows per page 10 1 /1 Go Total: 8
Status Device Name Vendor IP Address MAC Address Device Type Device Model
Up 350-157 Netgear 192.168.10.157 30:46:9a:1a:db:a8 Standalone AP WNDAP350
Up 620-162 Netgear 192.168.10.162 84:1b:5e:5c:58:a8 Standalone AP WNDAP620
Up 660-167 Netgear 192.168.10.167 84:1b:5e:5d:18:18 Standalone AP WNDAP660
Up Jimmy-620-168 Netgear 192.168.10.168 84:1b:5e:5c:5b:a8 Standalone AP WNDAP620
Up July17-660-163 Netgear 192.168.10.163 84:1b:5e:5d:fa:f8 Standalone AP WNDAP660
Down netgear648318 Netgear 192.168.10.166 00:24:b2:64:83:18 Standalone AP WG103
Down netgearA102E8 Netgear 192.168.10.156 c4:3d:c7:a1:02:e8 Standalone AP WNDAP360
Up netgearA623F8 Netgear 192.168.10.150 e0:91:f5:a6:23:f8 Standalone AP WNAP210
Select
Cancel

6. To filter the devices or SSIDs that are listed, click the **Show Filter** button.

   You can filter the devices by criteria such as name, IP address, location, and model. You can filter the SSIDs by criteria such as SSID name, device name, and device IP address.

   To hide the filter for SSIDs or devices, click the **Hide Filter** button.

   The following figure shows an example of a screen that displays when you filter by device IP address:

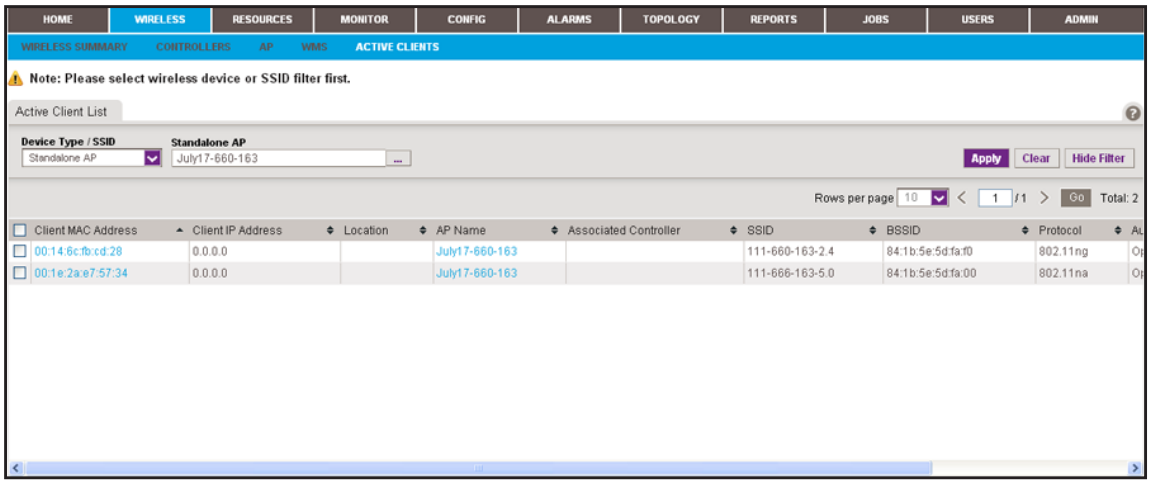


7. Select the device or SSID.
8. Click the **Select** button.

   The screen closes and the empty Active Client List table displays.

9. Click the **Apply** button.

The application populates the Active Client List table with the wireless clients of the selected device or SSID.

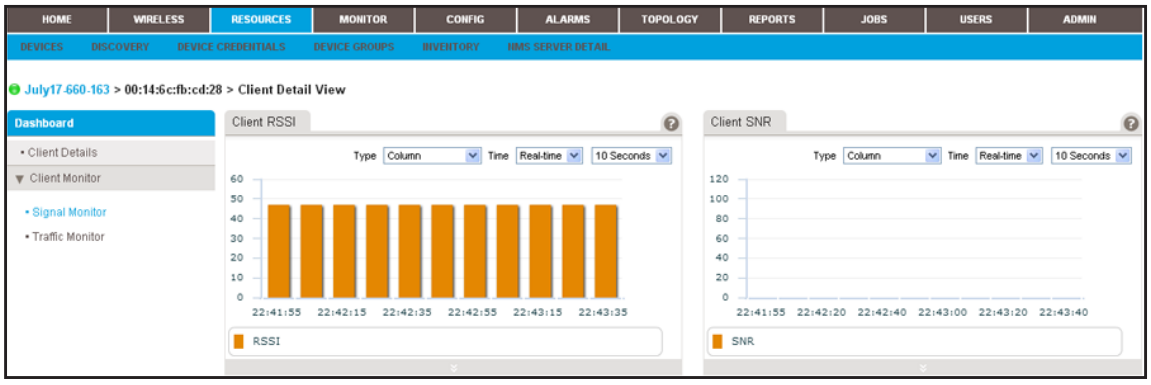


10. To add columns to or remove them from the Active Client List table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

    You can choose from the following columns: Client MAC Address, Client IP Address, Location, AP Name, Associated Controller, SSID, BSSID, Protocol, Authentication Mode, Duration, Channel, RSSI, SNR, Transmit Power, Transmitted, Rate (Mbps), Received Rate (Mbps), Transmitted Bytes, Received Bytes, Transmitted Packets, Received Packets, and Status.

11. To view details for an individual wireless client, in the Client MAC Address column, click a MAC address.

    A screen similar to the following displays.



12. From the **Dashboard** menu, select a menu option.

    By default, the screen displays the **Signal Monitor** menu option. If you select the **Traffic Monitor** menu option, the screen adjusts.

The following table lists some of the dashboard options and widgets or tables that are available for a wireless client.

Dashboard Option	Widget or Table
Signal Monitor	Client RSSI
	Client SNR
Traffic Monitor	Client Received/Transmitted Bytes
	Client Data Rate

Manage the Configuration Monitors

The application provides monitors for the following device metrics:

- Status
- ICMP ping
- CPU
- Memory
- Temperature
- IP traffic
- ICMP traffic
- TCP traffic
- UDP traffic
- SNMP traffic
- Interface traffic

In addition, the application provides monitors for the following server and wireless metrics:

- NMS300 server
- Radio statistics
- WLAN utilization
- VAP statistics (wireless performance statistics of the WLAN network based on SSID)
- Wired Ethernet statistics (wired performance statistics of standalone APs)

By default, all monitors are enabled. You can disable or reenable individual monitors and specify the information and devices that are monitored.

For information about how to configure alarm trigger settings for these monitors, see *Add a Custom Alarm Configuration* on page 148.

The following sections describe the tasks that you can perform for the configuration monitors:

- *Configure an Individual Monitor*
- *Disable a Monitor*
- *Reenable a Monitor*
- *View or Modify the Polling Interval for a Monitor*

Configure an Individual Monitor

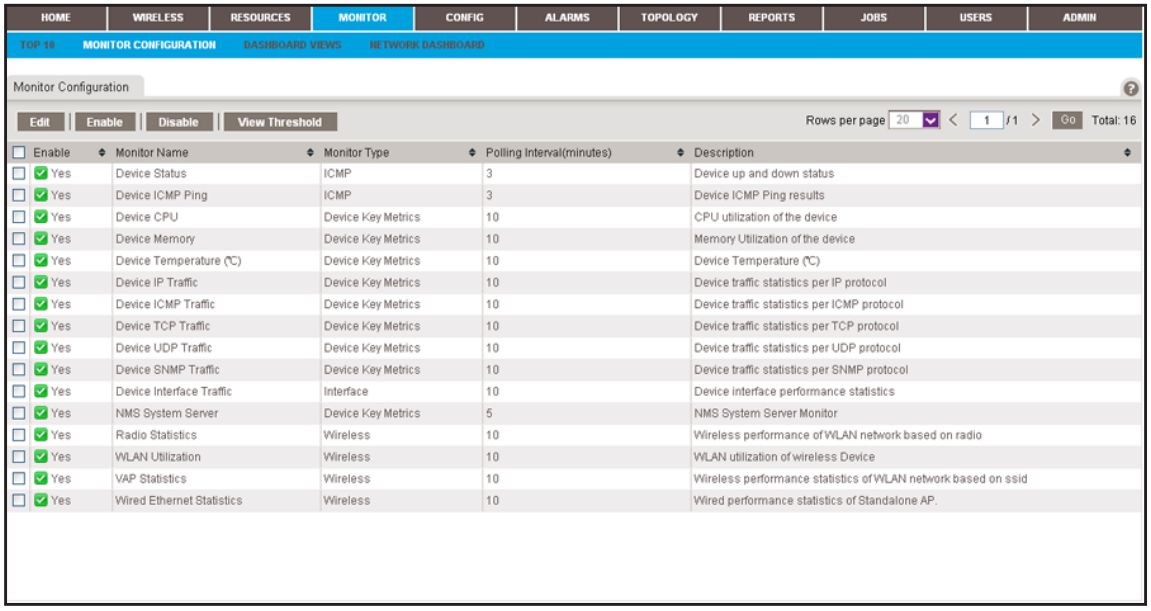
For each individual monitor, you can modify the information and devices that are monitored.

➢ **To configure an individual monitor:**

1. Log in to the application.

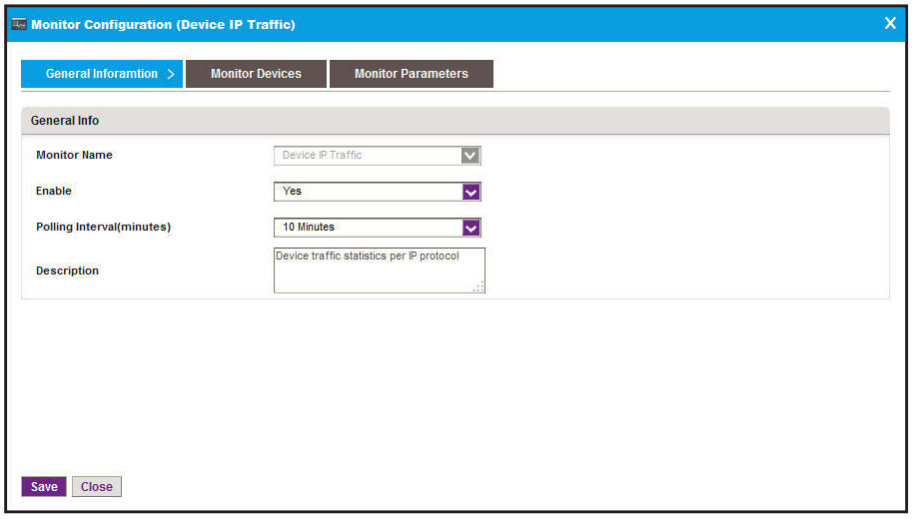
   For more information, see *Log In to the Application* on page 15.

2. Select **MONITOR > MONITOR CONFIGURATION**.

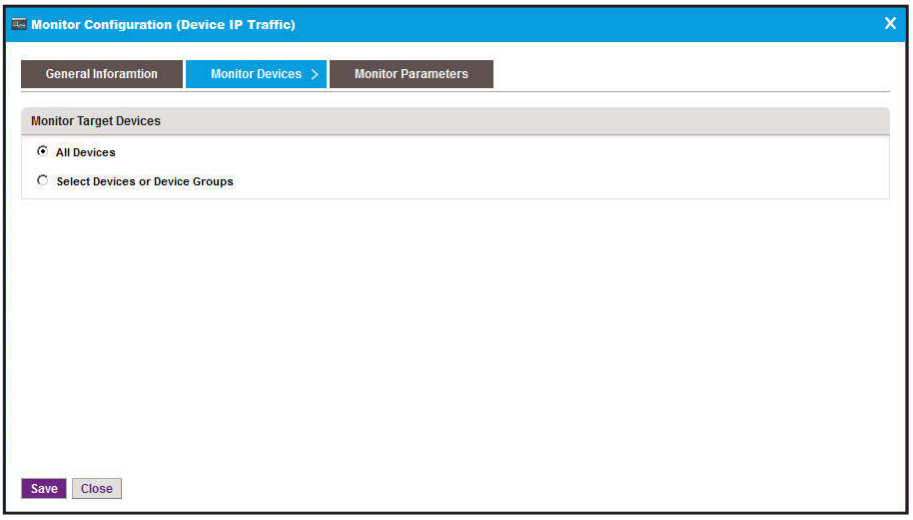

HOME
WIRELESS
RESOURCES
MONITOR
CONFIG
ALARMS
TOPOLOGY
REPORTS
JOBS
USERS
ADMIN
TOP 10
MONITOR CONFIGURATION
DASHBOARD VIEWS
NETWORK DASHBOARD
Monitor Configuration
Edit
Enable
Disable
View Threshold
Rows per page 20
1 /1
Go
Total: 16
Enable
Monitor Name
Monitor Type
Polling Interval(minutes)
Description
Yes Device Status ICMP 3 Device up and down status
Yes Device ICMP Ping ICMP 3 Device ICMP Ping results
Yes Device CPU Device Key Metrics 10 CPU utilization of the device
Yes Device Memory Device Key Metrics 10 Memory Utilization of the device
Yes Device Temperature (℃) Device Key Metrics 10 Device Temperature (℃)
Yes Device IP Traffic Device Key Metrics 10 Device traffic statistics per IP protocol
Yes Device ICMP Traffic Device Key Metrics 10 Device traffic statistics per ICMP protocol
Yes Device TCP Traffic Device Key Metrics 10 Device traffic statistics per TCP protocol
Yes Device UDP Traffic Device Key Metrics 10 Device traffic statistics per UDP protocol
Yes Device SNMP Traffic Device Key Metrics 10 Device traffic statistics per SNMP protocol
Yes Device Interface Traffic Interface 10 Device interface performance statistics
Yes NMS System Server Device Key Metrics 5 NMS System Server Monitor
Yes Radio Statistics Wireless 10 Wireless performance of WLAN network based on radio
Yes WLAN Utilization Wireless 10 WLAN utilization of wireless Device
Yes VAP Statistics Wireless 10 Wireless performance statistics of WLAN network based on ssid
Yes Wired Ethernet Statistics Wireless 10 Wired performance statistics of Standalone AP.

3. Select the monitor.

4. Click the **Edit** button.



5. (Optional) In the General Information screen, modify the following settings:
   - From the **Polling Interval** menu, select a polling interval.
   - Enter a description.
6. Click the **Monitor Devices** tab.



7. (Optional) In the Monitor Devices screen, select one of the following radio buttons:
   - **All Devices**. Monitors all devices.
   - **Select Devices or Device Groups**. The screen adjusts to let you select devices, device groups, or both to monitor:
     a. Click the **Add Device** button.
     b. Either select individual devices and click the click **Add Selection** button, or click the **Add All** button.

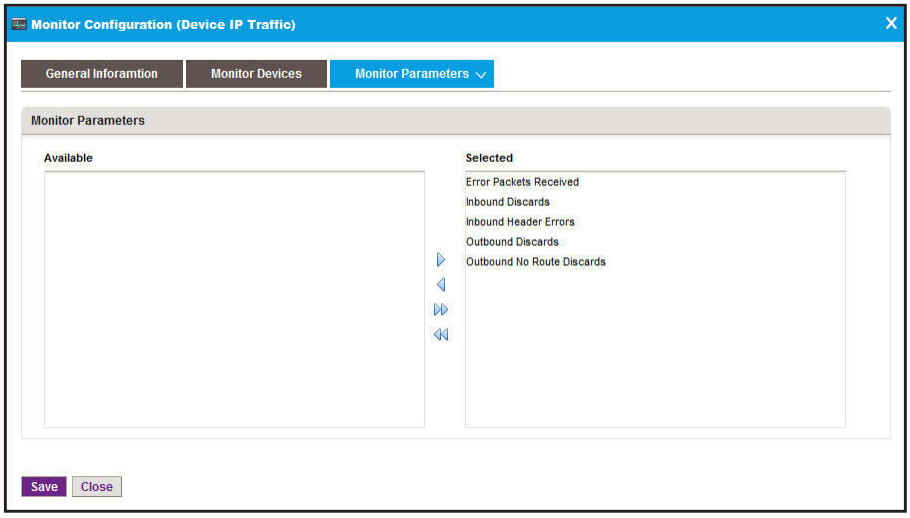
        The device or devices are added to the table on the Monitor Devices screen.

c. Click the **Add Group** button.

d. Either select individual devices and click the click **Add Selection** button, or click the **Add All** button.

The device groups or groups are added to the table on the Monitor Devices screen.

8. Click the **Monitor Parameters** tab.



9. (Optional) In the Monitor Devices screen, move parameters between the Available Fields table and Selected Fields table by using the **>**, **<**, **>>**, and **<<** buttons.

a. In the Available Fields table, select a parameter.

b. Click the **>** button.

The parameter moves to the Selected Fields table.

c. To move another parameter, repeat *Step a* and *Step b*.

10. Click the **Save** button.

Your changes are saved.

Disable a Monitor

By default, all monitors are enabled.

➢ **To disable a monitor:**

1. Log in to the application.

For more information, see *Log In to the Application* on page 15.

2. Select **MONITOR > MONITOR CONFIGURATION**.
3. Select the monitor.
4. Click the **Disable** button.

A pop-up confirmation screen displays.

5. Click the **Yes** button.

   The monitor is disabled. In the Monitor Configuration table, the Enable column displays No for the monitor.

Reenable a Monitor

➢ **To reenable a monitor after you disabled it:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **MONITOR > MONITOR CONFIGURATION**.
3. Select the monitor.
4. Click the **Enable** button.

   A pop-up confirmation screen displays.

   The monitor is reenabled. In the Monitor Configuration table, the Enable column displays Yes for the monitor.

View or Modify the Polling Interval for a Monitor

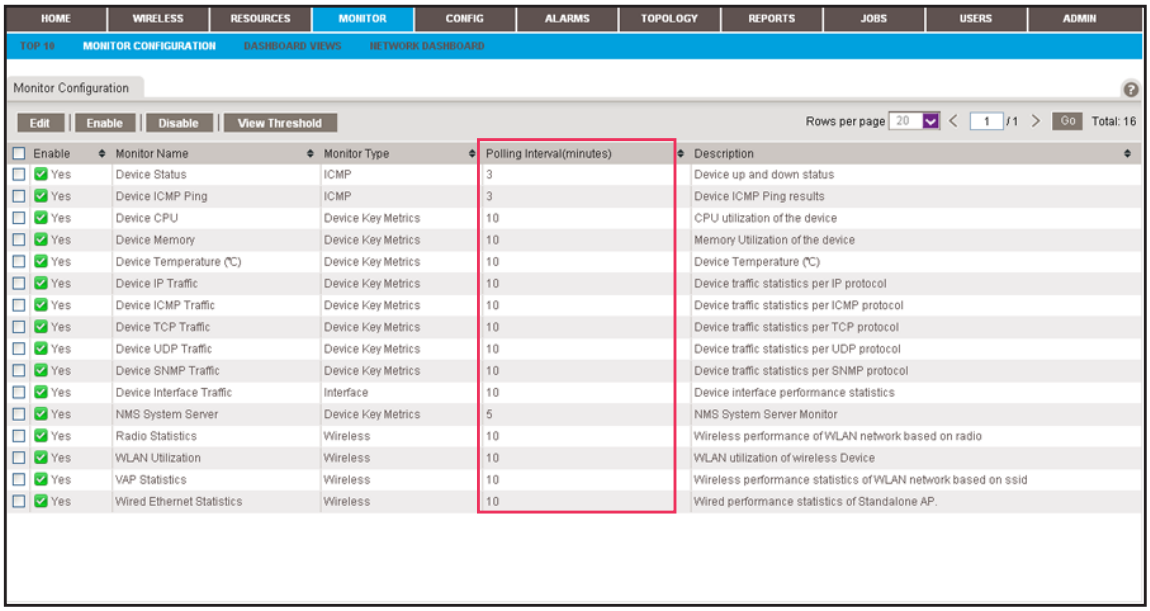
You can view and modify the polling interval for a monitor to control how frequently the device and network information is updated.

➢ **To view and modify the polling interval for a monitor:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **MONITOR > MONITOR CONFIGURATION**.


HOME
WIRELESS
RESOURCES
MONITOR
CONFIG
ALARMS
TOPOLOGY
REPORTS
JOBS
USERS
ADMIN
TOP 10
MONITOR CONFIGURATION
DASHBOARD VIEWS
NETWORK DASHBOARD
Monitor Configuration
Edit
Enable
Disable
View Threshold
Rows per page 20
1 /1
Go
Total: 16
Enable
Monitor Name
Monitor Type
Polling Interval(minutes)
Description
Yes Device Status ICMP 3 Device up and down status
Yes Device ICMP Ping ICMP 3 Device ICMP Ping results
Yes Device CPU Device Key Metrics 10 CPU utilization of the device
Yes Device Memory Device Key Metrics 10 Memory Utilization of the device
Yes Device Temperature (℃) Device Key Metrics 10 Device Temperature (℃)
Yes Device IP Traffic Device Key Metrics 10 Device traffic statistics per IP protocol
Yes Device ICMP Traffic Device Key Metrics 10 Device traffic statistics per ICMP protocol
Yes Device TCP Traffic Device Key Metrics 10 Device traffic statistics per TCP protocol
Yes Device UDP Traffic Device Key Metrics 10 Device traffic statistics per UDP protocol
Yes Device SNMP Traffic Device Key Metrics 10 Device traffic statistics per SNMP protocol
Yes Device Interface Traffic Interface 10 Device interface performance statistics
Yes NMS System Server Device Key Metrics 5 NMS System Server Monitor
Yes Radio Statistics Wireless 10 Wireless performance of WLAN network based on radio
Yes WLAN Utilization Wireless 10 WLAN utilization of wireless Device
Yes VAP Statistics Wireless 10 Wireless performance statistics of WLAN network based on ssid
Yes Wired Ethernet Statistics Wireless 10 Wired performance statistics of Standalone AP.

The current polling interval for each metric is listed on the screen in the Polling Interval (minutes) column.

3. Select the monitor.
4. Click the **Edit** button.
5. In the General Information screen, from the **Polling Interval** menu, select a polling interval.
6. Click the **Save** button.

   Your changes are saved.

Customize the Optional Network Dashboard

By default, the network dashboard does not display any information. If you want to use the network dashboard, you must create and customize network views and select one or more of these views on the network dashboard.

The following sections describe the network dashboard tasks:

- *Create or Modify a Dashboard View and Launch the Dashboard View*
- *Remove a Dashboard View*
- *Customize the Network Dashboard*

Create or Modify a Dashboard View and Launch the Dashboard View

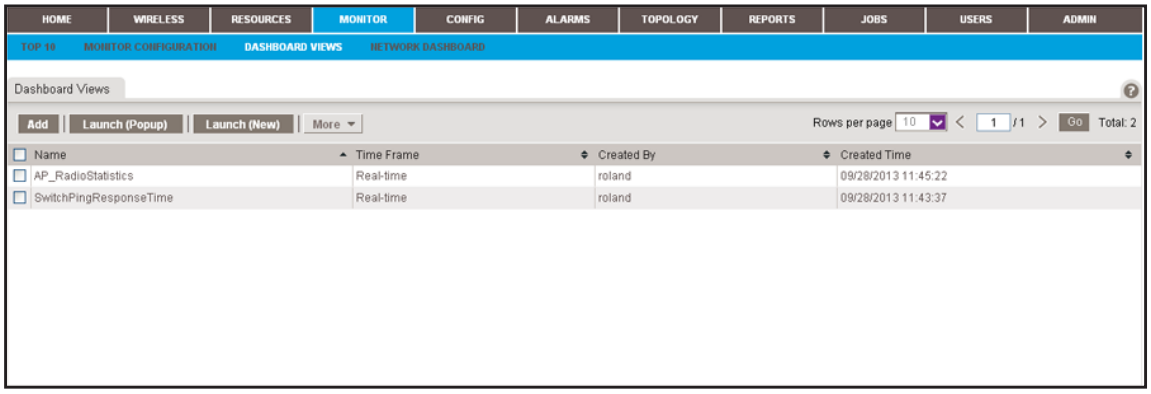
You can create dashboard views, including dashboard views that let you monitor performance in real time.

➢ **To create a dashboard view or modify an existing dashboard view and launch the dashboard view:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

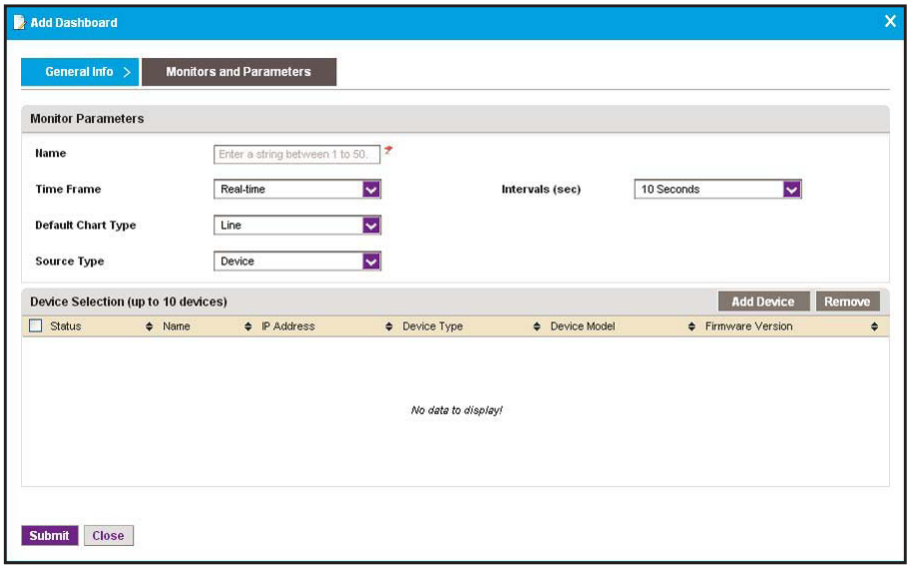
2. Select **MONITOR > DASHBOARD VIEWS**.



By default, the application does not include any dashboard views.

3. Create a dashboard view or modify an existing dashboard view:
   - To create a dashboard view, click the **Add** button.
   - To modify an existing dashboard view:
     a. From the Dashboard Views table, select the dashboard view.
     b. From the **More** menu, select **Edit**.

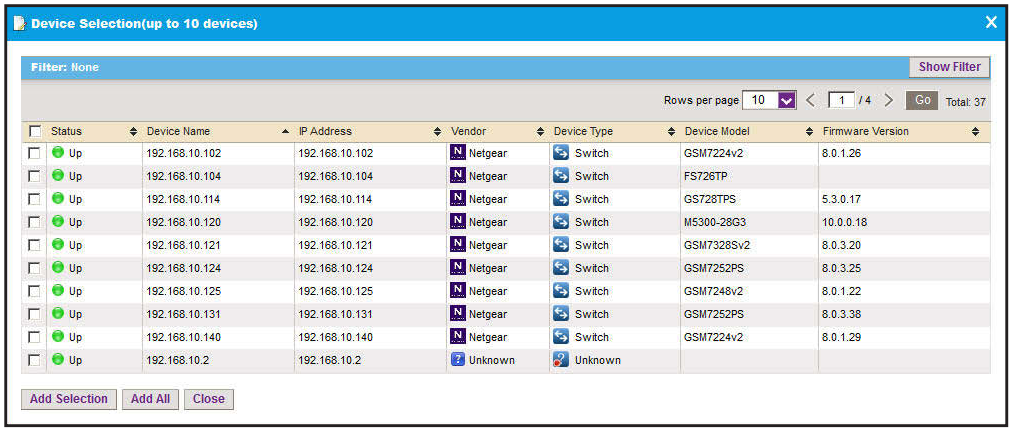
   For a new dashboard view, the Add Dashboard displays. For an existing dashboard view, the Edit Dashboard screen displays.



4. In the **Name** field, enter or modify the name for the dashboard view.
5. From the **Time Frame** menu, select the time frame over which you want to view the performance:
   - **Real-time**. View the performance in real time. (This is the default setting.) From the **Intervals (sec)** menu, select the period in seconds or minutes over which you want the view the performance:
     - **10 Seconds** (This is the default setting.)
     - **30 Seconds**
     - **1 Minute**
     - **2 Minutes**
     - **5 Minutes**
   - **Last Hour**
   - **Last 24 Hours**
   - **Last 7 Days**
   - **Last 30 Days**
6. If you select Real Time from the **Time Frame** menu, select a predefined period in seconds or minutes from the **Interval** menu.

7. From the **Default Chart Type** menu, select one of the following types:
   - **Line**
   - **Column**
   - **Column Stacked**
   - **Area**
   - **Area Stacked**
8. From the **Source Type** menu, select either **Device** or **Interface**:
   - **Device**. Create or modify a dashboard view of devices:
     a. Click the **Add Device** button.

        The Device Selection screen displays.

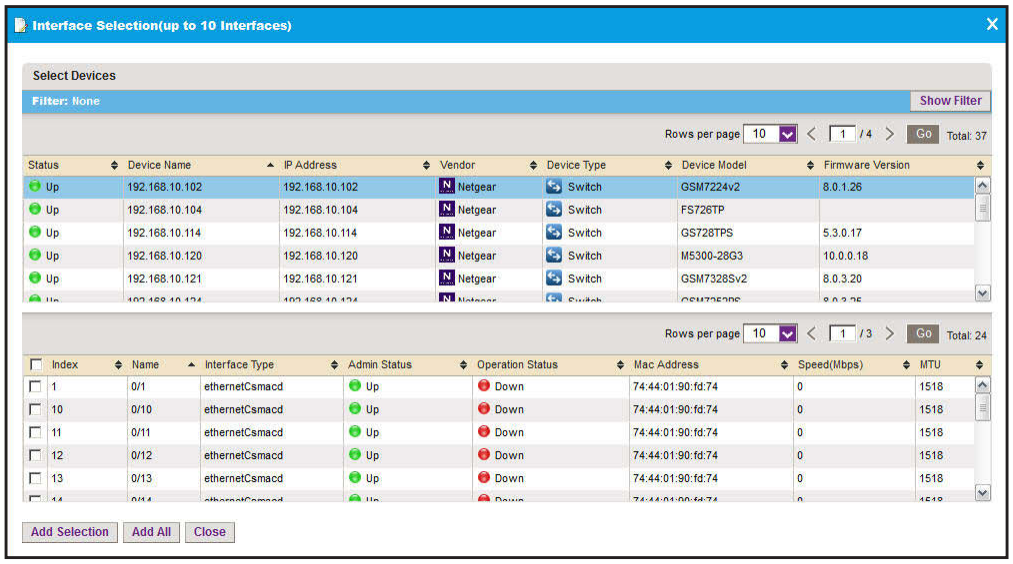


     b. To filter the devices that display in the table, click the **Show Filter** button.
     c. Select up to 10 devices and click the **Add Selection** button.

        To add the first 10 devices that display in the table, click the **Add All** button.
     d. If you are modifying an existing dashboard view, to remove devices, select the devices, and click the **Remove** button.

        The devices are removed from the Device Selection table.
   - **Interface**. Create or modify a dashboard view of interfaces:
     a. Click the **Add Interface** button.

        The Interface Selection screen displays.



b. To filter the devices that appear in the table, click the **Show Filter** button.

c. From the upper table, select a device for which you want to monitor interfaces.

d. From the lower table, select the interfaces, and click the **Add Selection** button.

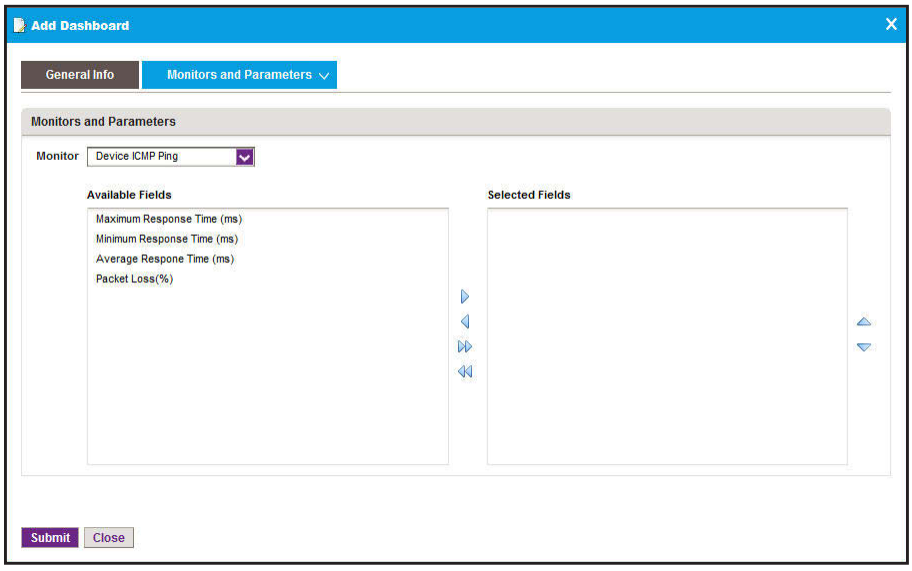
To add the first 10 interfaces that display in the table, click the **Add All** button.

e. To add interfaces for another device, repeat *Step a* through *Step d*.

f. If you are modifying an existing dashboard view, to remove interfaces, select the interfaces, and click the **Remove** button.

The interfaces are removed from the Interface Selection table.

9. Click the **Monitors and Parameters** tab.



10. From the **Monitor** menu, select a monitor.

The **Monitor** menu displays only common monitors that apply to the device types that you select in *step 8* on page 90. Your selection from the **Monitor** menu determines the options that display in the Available Fields section.

11. Specify the fields and their order.

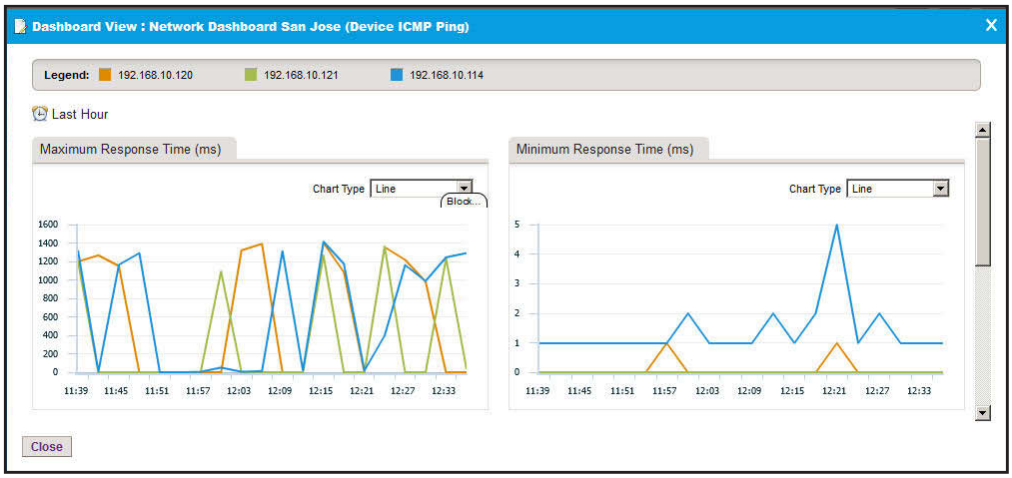
    To select the fields, use the left and right arrows. To arrange their order, use the up and down arrows.

12. Click the **Submit** button.

    The screen closes. The new or modified dashboard displays in the Dashboard Views table.

13. Select the new or modified dashboard view.
14. Click one of the following buttons:

- **Launch (Popup)**. A pop-up screen similar to the following displays.



  To close the screen, click the **X** (X) button.

- **Launch (New)**. A screen opens in a new browser window.

  The information that displays if you click the **Launch (New)** button is identical to the information that displays if you click the **Launch (Popup)** button.

Remove a Dashboard View

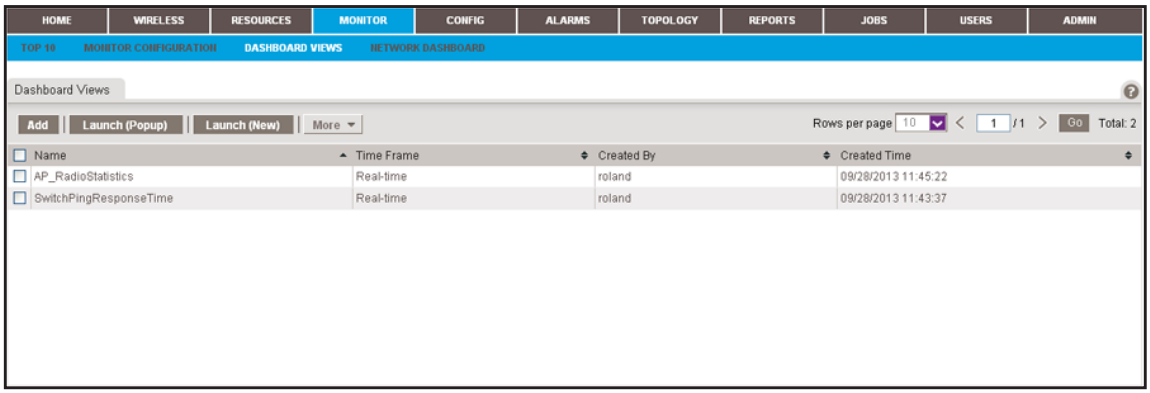
You can remove a dashboard view that you no longer need.

➢ **To remove a dashboard view:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **MONITOR > DASHBOARD VIEWS**.



3. Select the dashboard view.
4. From the **More** menu, select **Delete**.

   A pop-up confirmation screen displays.

5. Click the **Yes** button.

   The dashboard view is removed from the Dashboard Views table and deleted.

Customize the Network Dashboard

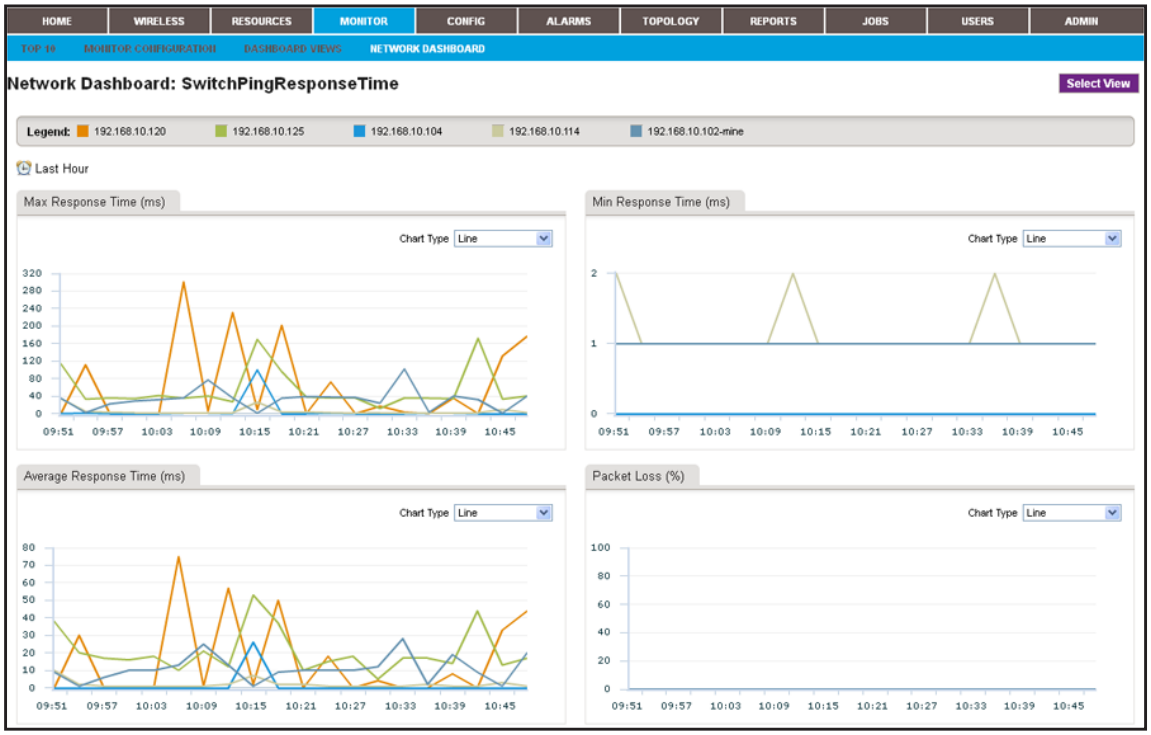
If you did not add any dashboard views (see *Create or Modify a Dashboard View and Launch the Dashboard View* on page 88), the network dashboard does not display any information. After you have added one or more dashboard views, you can select a dashboard view to display on the network dashboard.

➢ **To customize the network dashboard:**

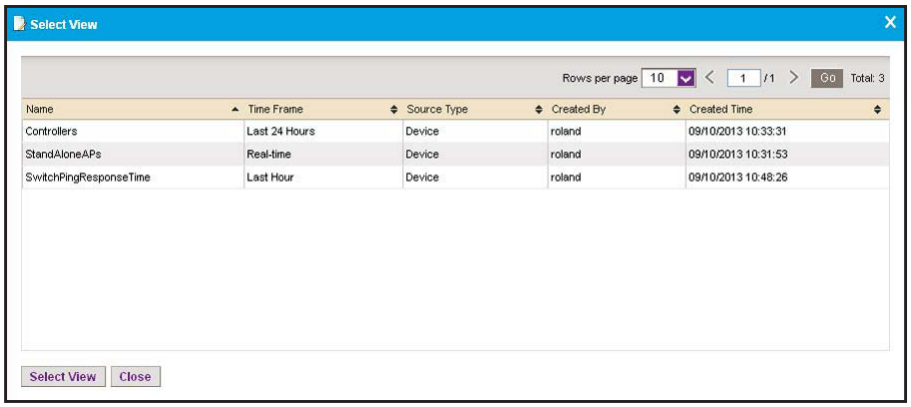
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **MONITOR > NETWORK DASHBOARD**.



3. Click the **Select View** button.



If the table does not display any dashboard views, you have not created any. For information about creating a dashboard view, see *Create or Modify a Dashboard View and Launch the Dashboard View* on page 88.

4. In the table, click the dashboard view.
5. Click the **Select View** button.

The screen closes and the selected network dashboard view displays.

View and Export Audit Logs

The system audit logs provide information about the tasks that you performed on the network or on the NMS300 server.

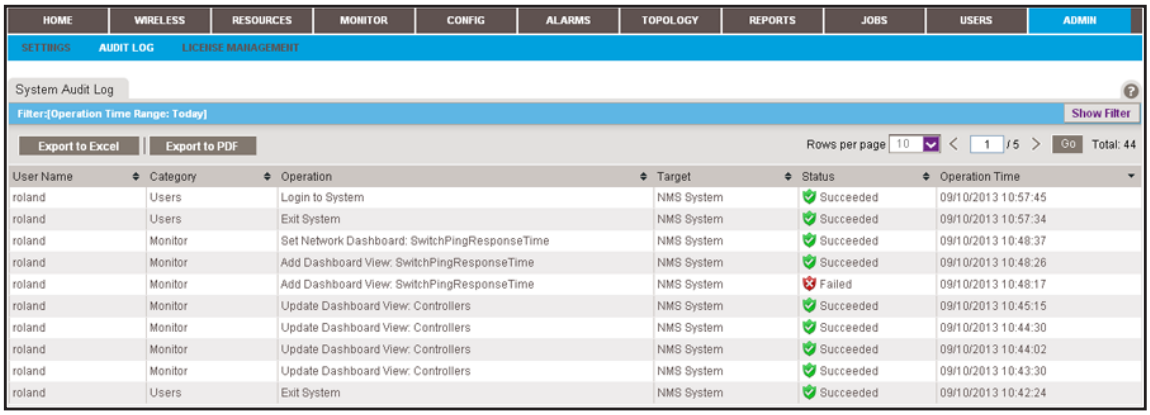
Audit logs are saved for the data retention period. For more information, see *Set the Data Retention Period* on page 214.

➢ **To view and export the application audit logs:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > AUDIT LOG**.



3. To filter the log entries that display in the System Audit Log table, click the **Show Filter** button.

   You can filter the log entries in the System Audit Log table by criteria such as user name, category, and operation time span.

   To hide the filter, click the **Hide Filter** button.

4. Click the **Export to Excel** button or the **Export to PDF** button.
5. To save the audit logs on your computer, follow the directions of your browser.

View Firmware Version Information

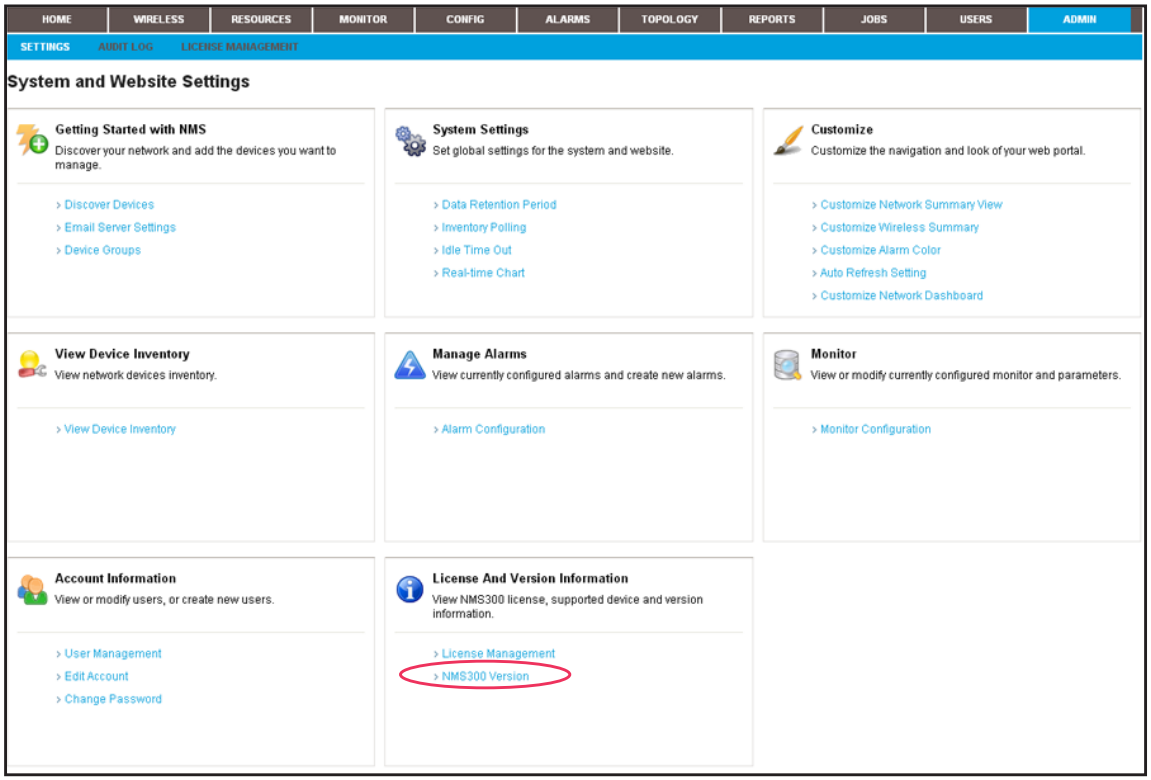
You can view the firmware version information for the application and for all NETGEAR switches, NETGEAR wireless devices, and NETGEAR firewalls that the application discovered.

➢ **To view firmware version information:**

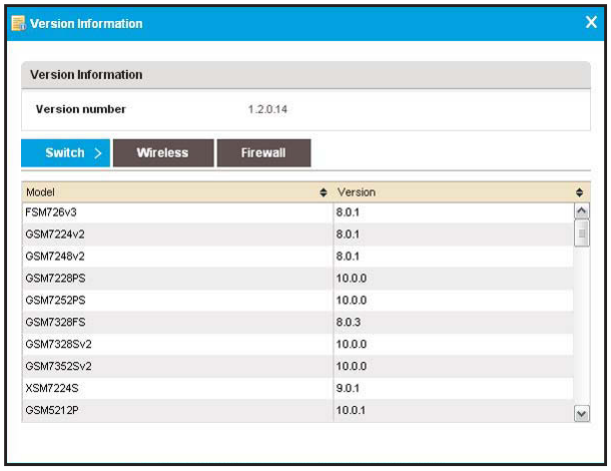
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under License And Version Information, click the **NMS300 Version** link.



Under Version Information, the firmware version of the application displays in the **Version number** field.

4. To view firmware versions of NETGEAR devices that the application discovered, click the **Switch**, **Wireless**, or **Firewall** tab.
5. Click the **X** (X) button.

   The screen closes.

View the NMS300 Server Information

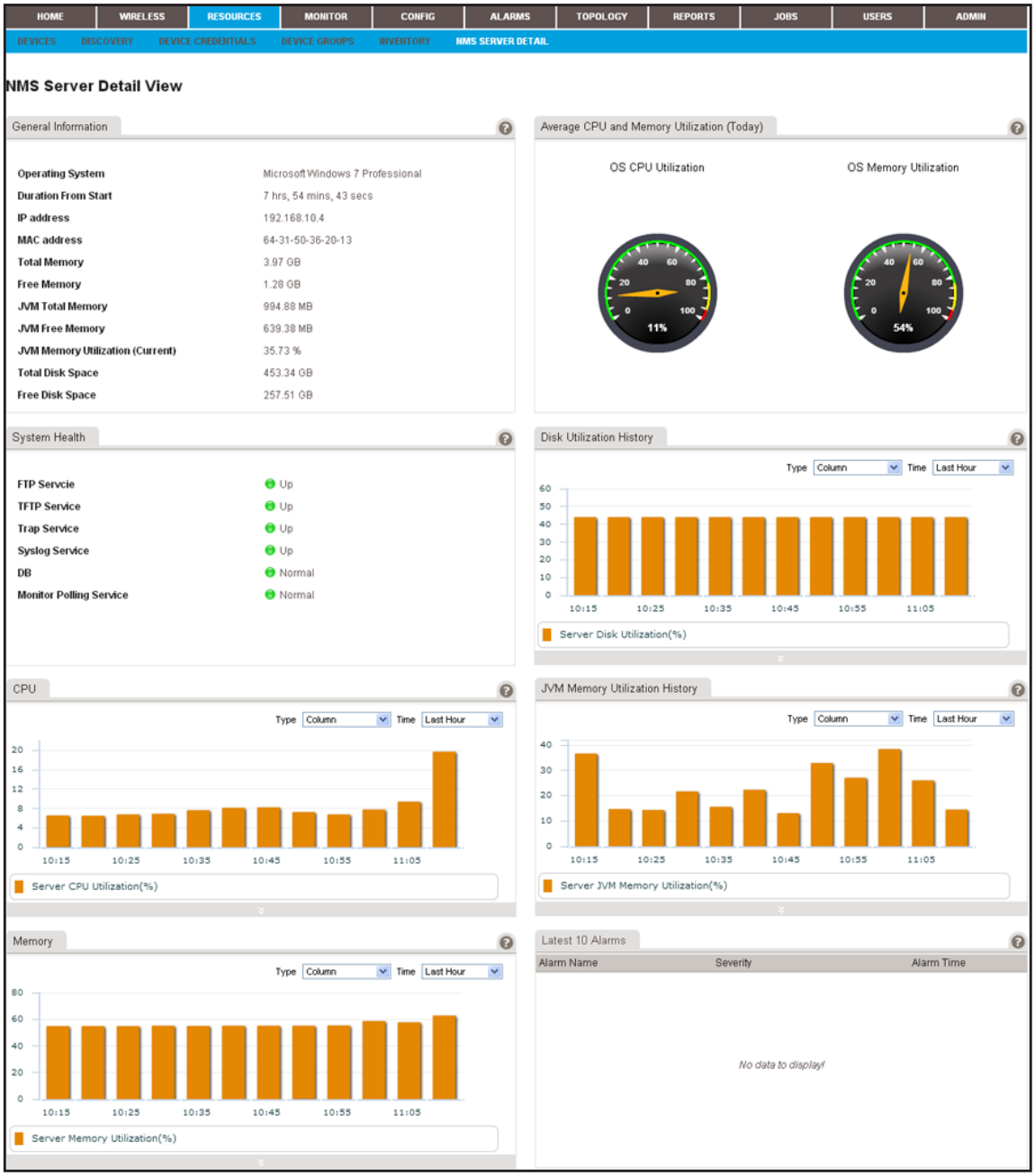
You can monitor the performance information of the NMS300 server.

➢ **To view the NMS300 server information:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **RESOURCES > NMS SERVER DETAIL**.



View Application Notifications

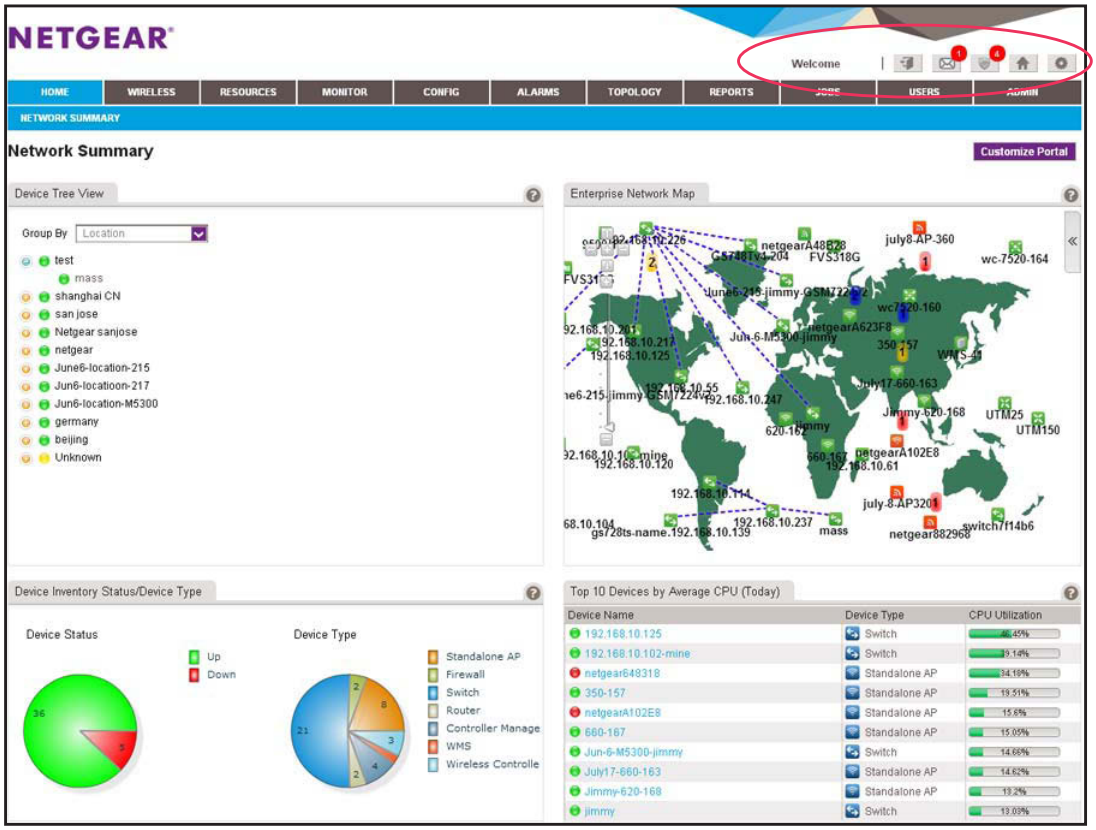
The application generates a notification when a task is completed. For example, if you have initiated a firmware upgrade for one or more devices, the application generates a notification when the upgrade is completed. The notification includes details about whether the task completed successfully.

When the application generates one or more notifications, a small red-colored circle displays on top of the **Envelope** button in the top bar at the upper right of the screen. A number in the circle indicates the number of notifications that the application generated.

➢ **To view application notifications:**

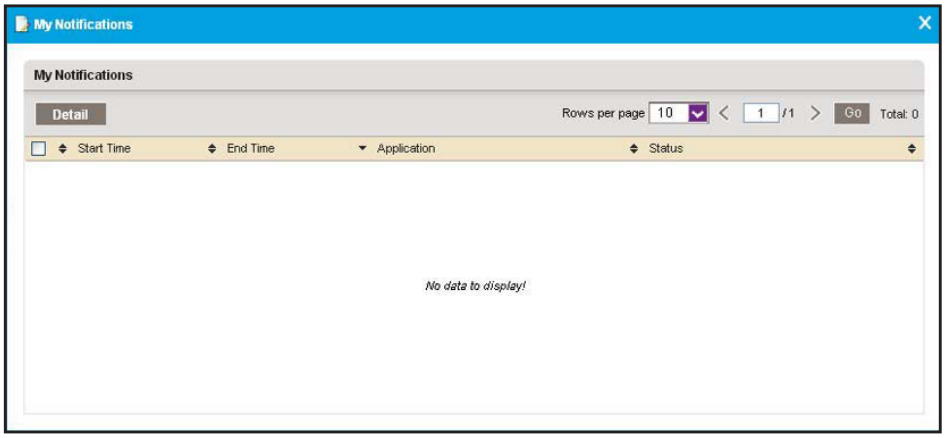
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.



2. In the top bar at the upper right of the screen, click the **Envelope** button.

The My Notifications screen displays.



3. To view details about a notification, select the notification and click the **Details** button.
4. To close the screen, click the **X** ( ) button.

Manage Configurations and Firmware

5

Keep your device firmware current

You can back up and restore device configurations. You can also upgrade device firmware.

This chapter covers the following topics:

- *Back Up Your Device Configurations*
- *Restore Your Device Configurations*
- *Upgrade Firmware for One or More Devices*

Back Up Your Device Configurations

You can back up the configurations of the NETGEAR devices on your network.

You can schedule configuration backup jobs for future execution on a recurrent basis for batch operations.

The following sections describe the backup tasks:

- *Add or Modify a Backup Profile*
- *Execute a Backup Job*
- *Schedule a Backup Job*
- *View the Execution Status of a Backup Job*
- *Remove a Backup Profile*

Add or Modify a Backup Profile

A backup profile defines the devices that are included in a backup job, and as an option, the schedule with which the backup job occurs. You must create a backup profile before you can back up the configuration of one or more devices.

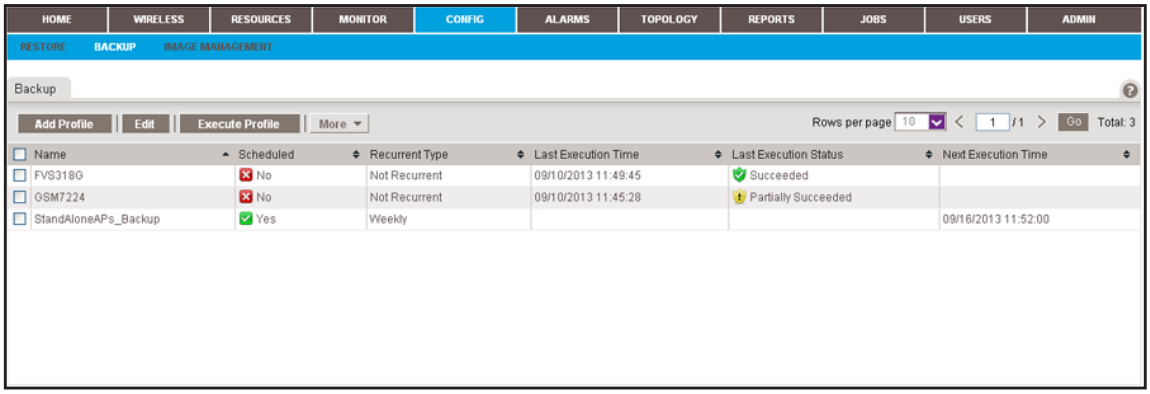
To a single backup profile, you can add devices, device groups, or both.

➢ **To add a backup profile or modify an existing backup profile:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > BACKUP**.



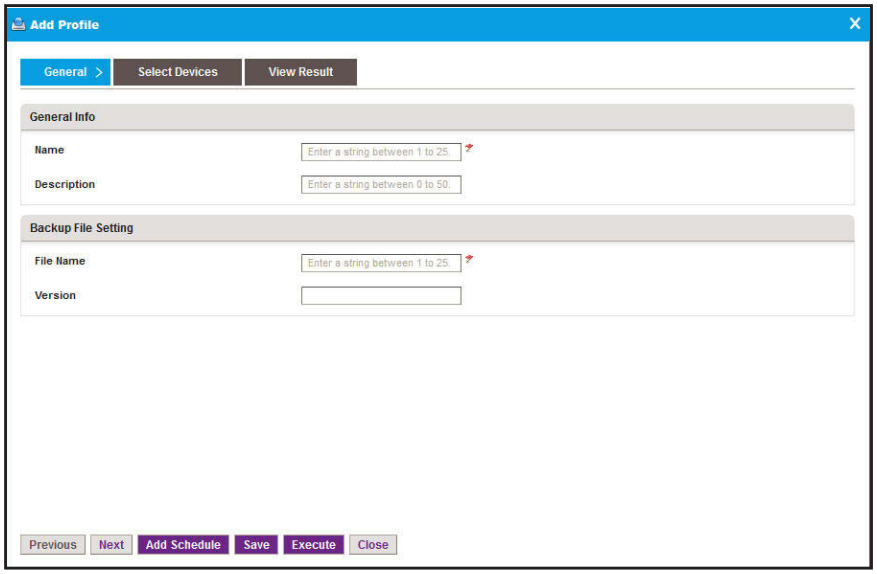
   The Backup screen displays the existing backup profiles.

3. To add columns to or remove them from the Backup table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

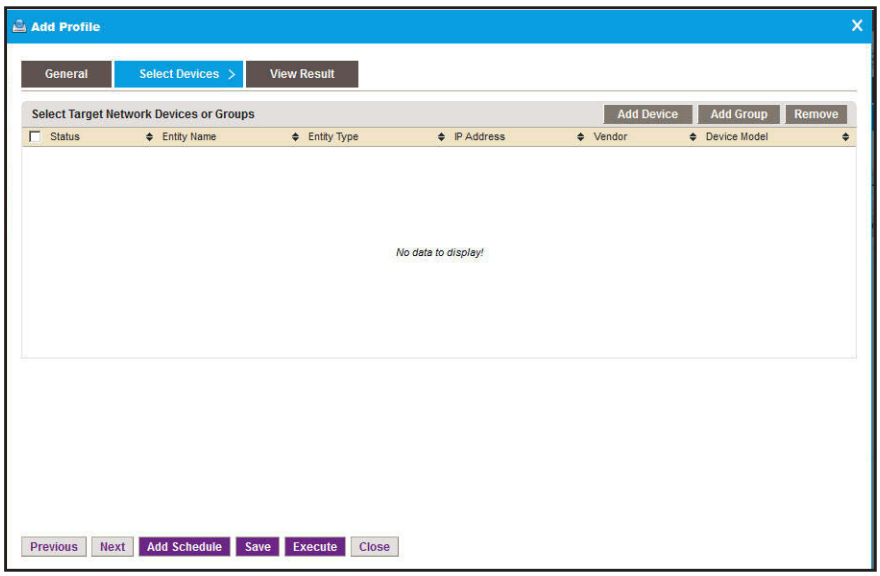
   You can choose from the following columns: Name, Scheduled, Recurrent Type, Last Execution Time, Last Execution Status, Next Execution Time, Description, Created By, and Created Time.

4. Add a backup profile or modify an existing backup profile:
   - To add a backup profile, click the **Add Profile** button.
   - To modify an existing backup profile:
     a. From the Backup table, select a backup profile.
     b. Click the **Edit** button.

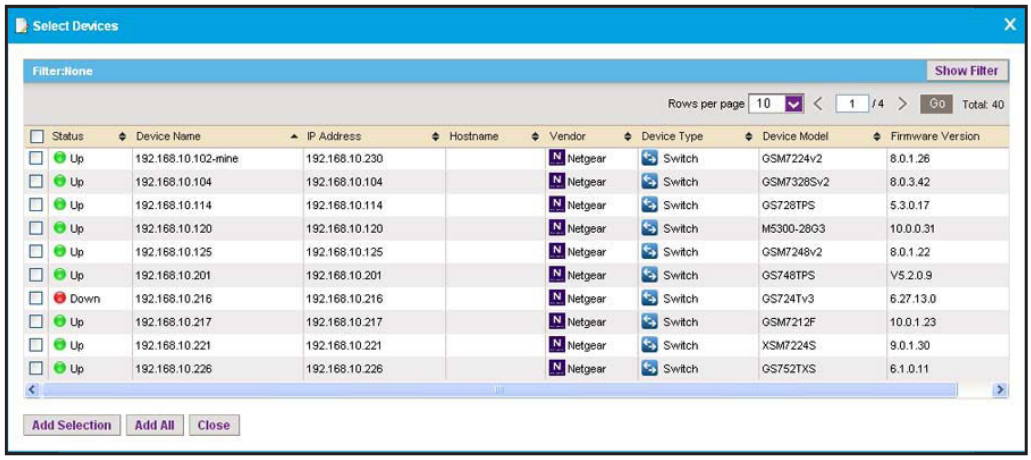
   For a new backup profile, the Add Profile screen displays. For an existing backup profile, the Edit Profile screen displays.



5. Enter or modify the following information:
   - **General Info**. Enter a name and description for the new profile.
   - **Backup File Setting**. Enter a file name and version for the backup file.
6. Click the **Select Devices** tab.



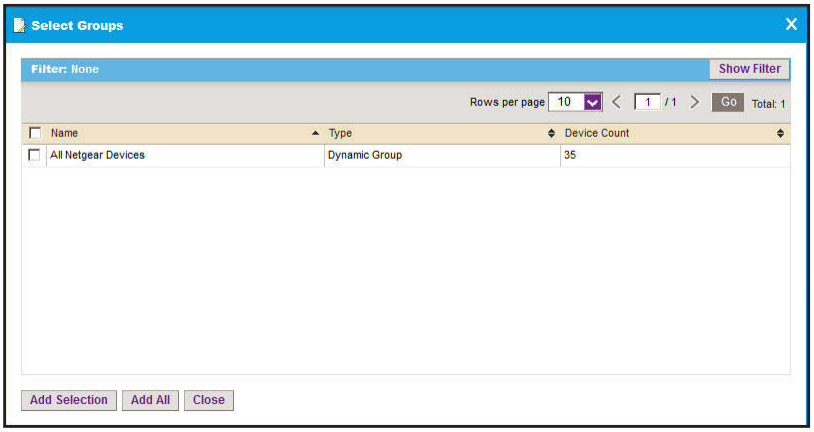
7. Add devices, device groups, or both:
   a. Click the **Add Device** button.



   b. Select devices to add and click the **Add Selection** button.

      To add all of the devices in the table, click the **Add All** button.

   c. Click the **Add Group** button.



   d. Select device groups to add and click the **Add Selection** button.

      To add all of the device groups in the table, click the **Add All** button.

   The selected devices, groups, or both, display in the Select Target Network Devices or Groups table.

8. If you are modifying an existing backup profile, to remove devices or groups:
   a. Select the devices or groups.
   b. Click the **Remove** button.

   The devices or groups are removed from the Select Target Network Devices or Groups table.

9. To add a schedule, click the **Add Schedule** button.

You can schedule the generation of the report for a later time or have it recur automatically. For more information, see *Schedule a Backup Job* on page 105.

10. Click the **Save** button.

    The new or modified backup profile is saved and displays in the Backup screen.

11. To execute the backup job, click the **Execute** button.

    Your backup profile is executed immediately.

Execute a Backup Job

You can execute a one-time backup profile immediately. Executing a backup profile is referred as a backup job.

The application saves the backup configuration files on the NMS300 server and lists them on the Restore screen. You can use the backup files to restore device configurations for the devices on your network. For more information, see *Restore Your Device Configurations* on page 110.

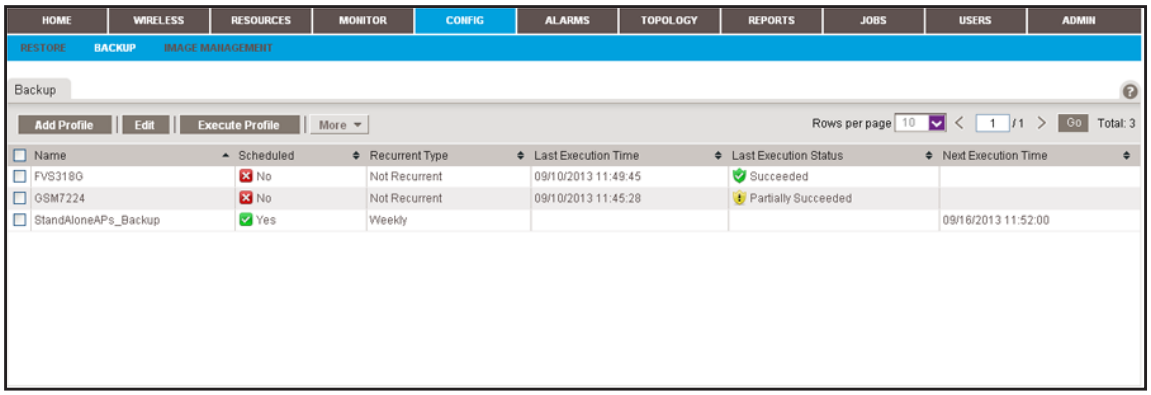
The application saves configuration files from completed backup jobs for the data retention period. For more information, see *Set the Data Retention Period* on page 214.

➢ **To execute a backup profile immediately:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > BACKUP**.



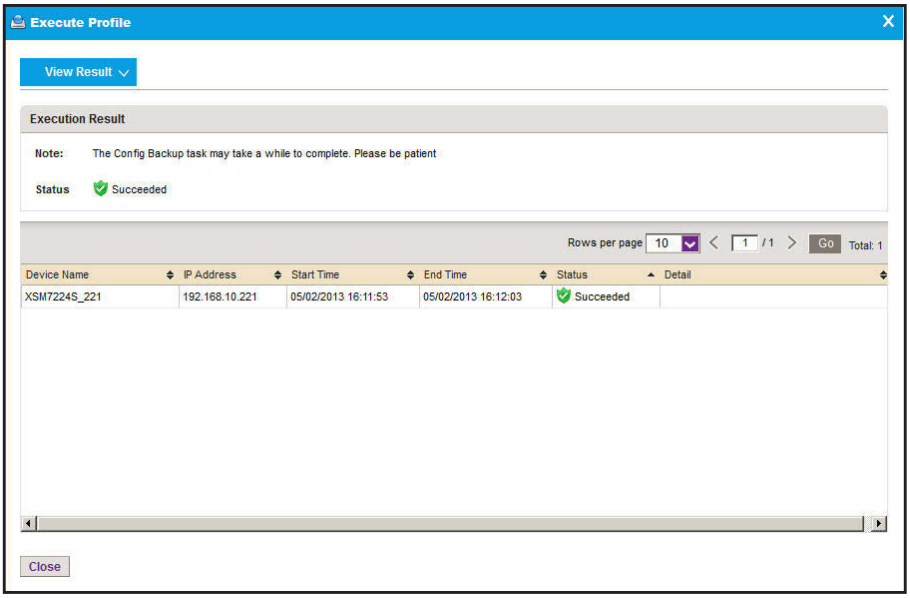
   The Backup screen displays the existing backup profiles in the application.

3. To add columns to or remove them from the Backup table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Name, Scheduled, Recurrent Type, Last Execution Time, Last Execution Status, Next Execution Time, Description, Created By, and Created Time.

4. Select the backup profile.

5. Click the **Execute Profile** button.


Execute Profile
View Result
Execution Result
Note: The Config Backup task may take a while to complete. Please be patient
Status Succeeded
Rows per page 10 1 /1 Go Total: 1
Device Name IP Address Start Time End Time Status Detail
XSM7224S_221 192.168.10.221 05/02/2013 16:11:53 05/02/2013 16:12:03 Succeeded
Close

The **Status** field displays the progress of the backup job. After the job completes successfully, the **Status** field displays **Succeeded**.

6. Click the **Close** button.

The screen closes.

Schedule a Backup Job

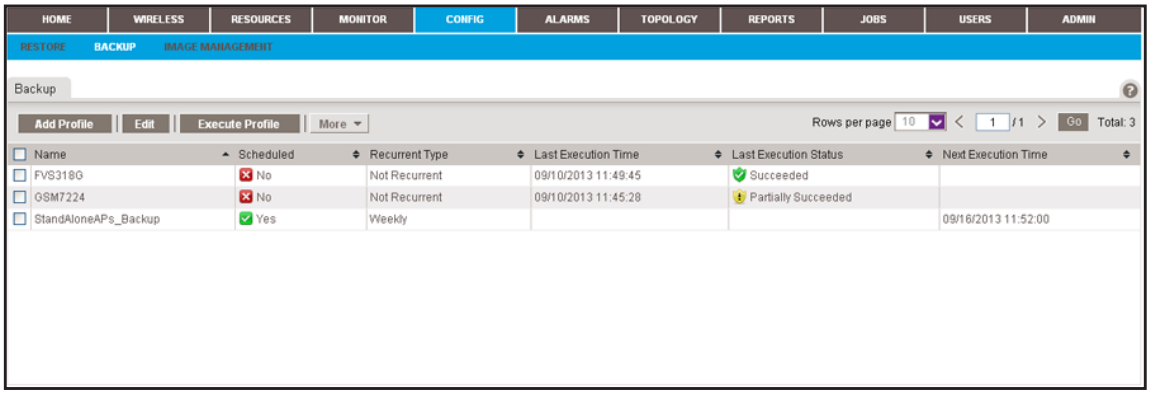
You can schedule a backup job to occur later, either once or on a recurring basis.

➢ **To schedule a backup job:**

1. Log in to the application.

For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > BACKUP**.

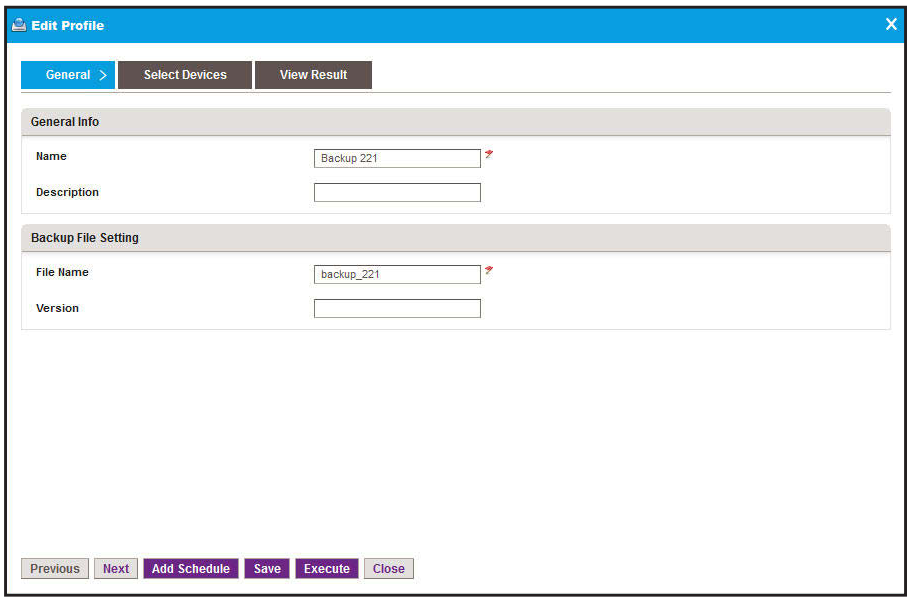

HOME WIRELESS RESOURCES MONITOR CONFIG ALARMS TOPOLOGY REPORTS JOBS USERS ADMIN
RESTORE BACKUP IMAGE MANAGEMENT
Backup
Add Profile Edit Execute Profile More
Rows per page 10 1 /1 Go Total: 3
Name Scheduled Recurrent Type Last Execution Time Last Execution Status Next Execution Time
FVS318G No Not Recurrent 09/10/2013 11:49:45 Succeeded
GSM7224 No Not Recurrent 09/10/2013 11:45:28 Partially Succeeded
StandAloneAPs_Backup Yes Weekly 09/16/2013 11:52:00

The Backup screen displays the existing backup profiles in the application.

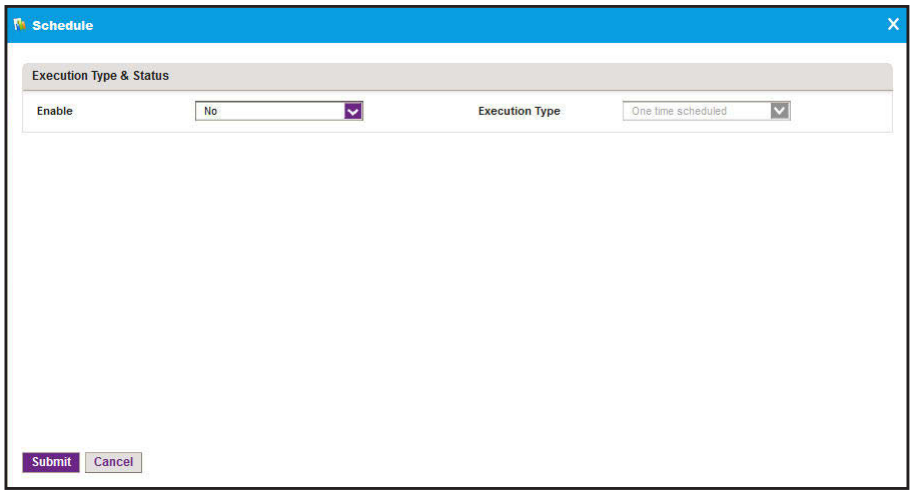
3. To add columns to or remove them from the Backup table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Name, Scheduled, Recurrent Type, Last Execution Time, Last Execution Status, Next Execution Time, Description, Created By, and Created Time.

4. Select the backup profile.
5. Click the **Edit** button.



6. Click the **Add Schedule** button.



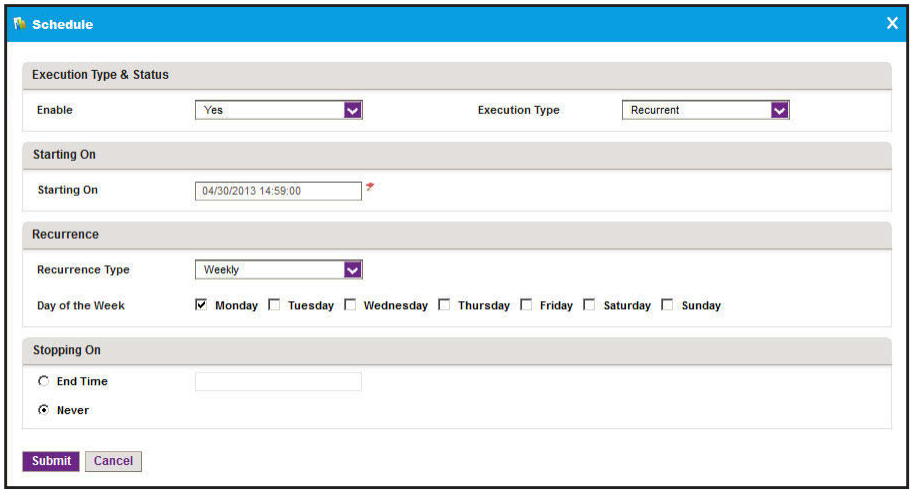
7. From the **Enable** menu, select **Yes**.

8. Specify whether the application executes the backup job once or on a recurring basis by selecting one of the following options from the **Execution Type** menu and entering the corresponding information:

   - **One time scheduled**. This is the default selection.

     In the **Starting On** field, enter a date and time.

   - **Recurrent**. The screen adjusts to display more fields.



   Enter the following information:

   a. In the **Starting On** field, enter a date and time.
   b. From the **Recurrence Type** menu, select how the schedule recurs and complete the corresponding field or select the corresponding check boxes.
   c. Select the **End Time** radio button and enter the date and time in the corresponding field, or leave the **Never** radio button selected, which is the default setting.

9. Click the **Submit** button.

   The Schedule screen closes. The backup job schedule becomes part of the backup profile.

10. On the Edit Profile screen, click the **Save** button.

    The backup job is executed according to the schedule that you set.

The application saves the backup configuration files on the NMS300 server and lists them on the Restore screen. You can use the backup files to restore device configurations for the devices on your network. For more information, see *Restore Your Device Configurations* on page 110.

The application saves configuration files from completed backup jobs for the data retention period. For more information, see *Set the Data Retention Period* on page 214.

View the Execution Status of a Backup Job

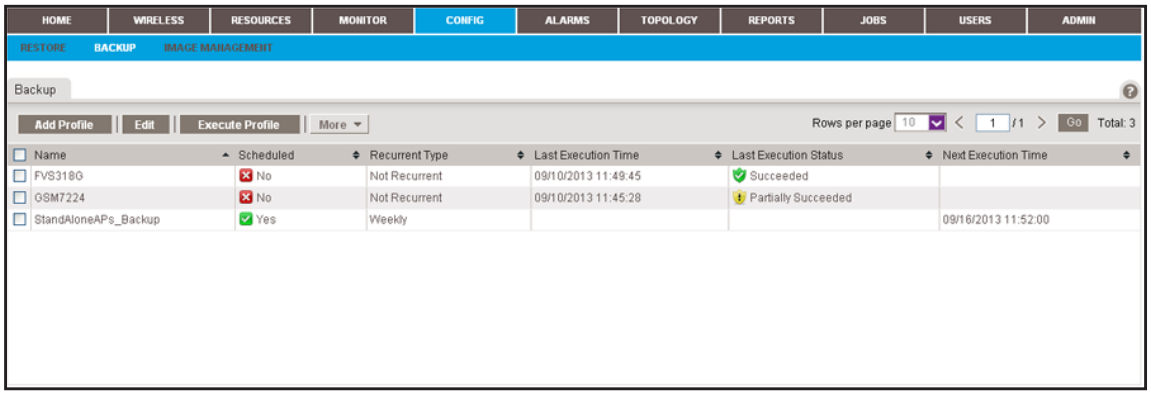
You can view the execution status of a backup job to ensure that a device configuration was backed up as scheduled.

➢ **To view the status of a backup job:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > BACKUP**.

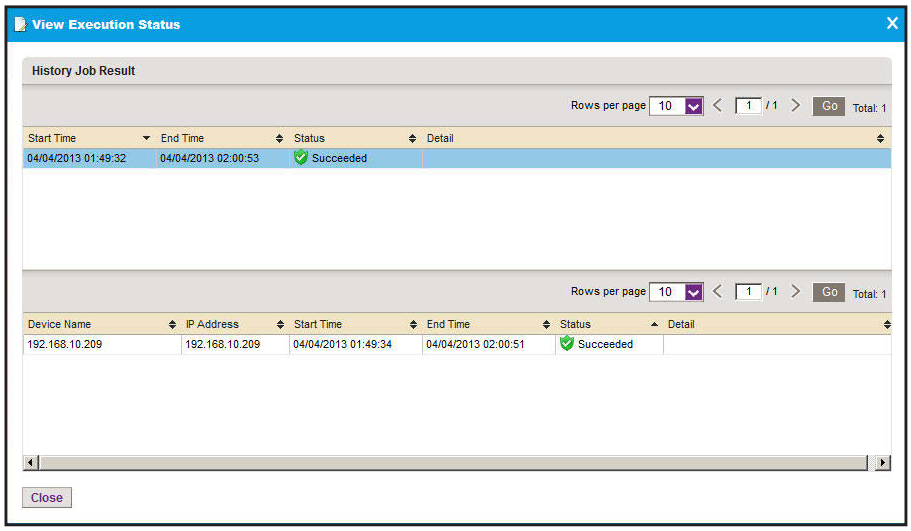


   The Backup screen displays the existing backup profiles in the application.

3. To add columns to or remove them from the Backup table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Name, Scheduled, Recurrent Type, Last Execution Time, Last Execution Status, Next Execution Time, Description, Created By, and Created Time.

4. Select the backup profile.
5. From the **More** menu, select **View Execution Status**.



The screen displays the execution history of a job and whether the job succeeded or failed.

6. Click the **Close** button.

   The screen closes.

Remove a Backup Profile

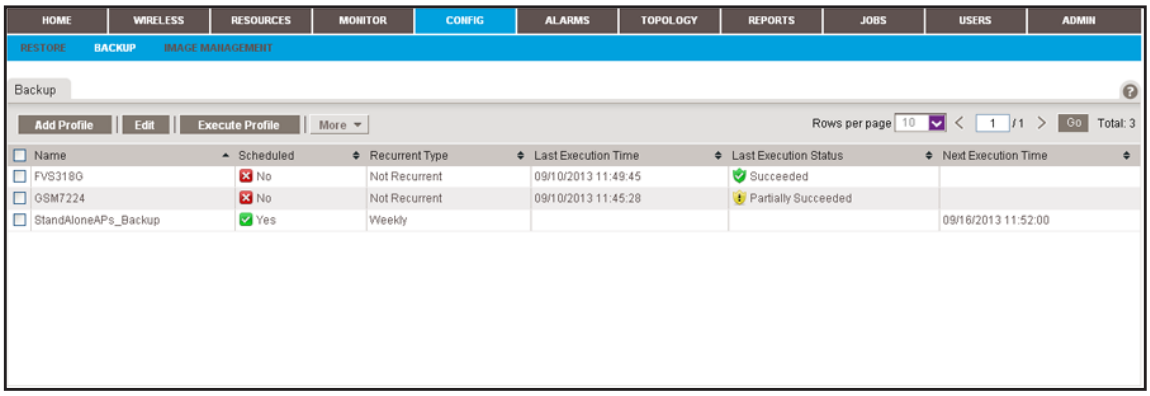
If you delete a backup job from the Jobs table, the application deletes the backup profile for the job automatically. For more information, see *View and Manage Jobs* on page 202. You can also remove a backup profile manually.

➢ **To remove a backup profile manually:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > BACKUP**.



3. To add columns to or remove them from the Backup table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Name, Scheduled, Recurrent Type, Last Execution Time, Last Execution Status, Next Execution Time, Description, Created By, and Created Time.

4. Select the backup profile.
5. From the **More** menu, select **Delete Profile**.

   A pop-up confirmation screen displays.

6. Click the **Yes** button.

   The backup profile is removed from the Backup table and deleted.

Restore Your Device Configurations

You can restore the configurations of the devices that the application manages on your network, as follows:

- **Single device**. You can restore the configuration of a single device on your network. For more information, see *Restore the Configuration of a Single Device* on page 111.
- **Several identical devices**. You can use the configuration of one of the devices on your network to create a configuration template for several identical devices on your network. For more information, see *Customize and Promote a Configuration File* on page 114 or *Promote a Configuration File for Firewalls* on page 117 and *Restore the Configuration of Several Identical Devices* on page 120.

The Restore table (which you access by selecting **CONFIG > RESTORE**) displays the backup configuration files that the application adds after it has backed up a configuration.

The application saves backup configuration files for the data retention period. For more information, see *Set the Data Retention Period* on page 214.

If the configuration file that you need does not display in the Restore table, you can import the file into the application. For more information, see *Import a Configuration File* on page 125. The Restore table also displays the configuration files that you imported.

CAUTION:

When you restore the configuration of a device, you must provide the correct configuration file. Make sure that you select both the correct device type and correct device model for the configuration file that you upload to the application. If you provide the wrong configuration file, the application pushes the incorrect configuration file when it executes the configuration restore job and you can damage the device.

The following sections describe the tasks that you can perform with device configuration files:

- *Restore the Configuration of a Single Device*
- *Customize and Promote a Configuration File*
- *Promote a Configuration File for Firewalls*
- *Restore the Configuration of Several Identical Devices*
- *Import a Configuration File*
- *Export a Configuration File*
- *Modify a Configuration File*
- *Remove a Configuration File*
- *Compare Two Configuration Files*

Restore the Configuration of a Single Device

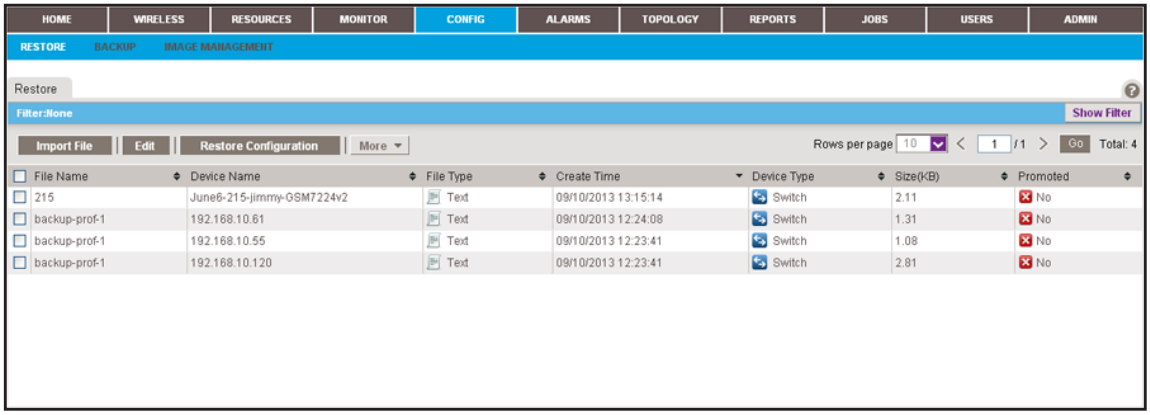
You can restore the configuration of a single device immediately or schedule the application to restore the configuration later.

➢ **To restore a configuration to a single device:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

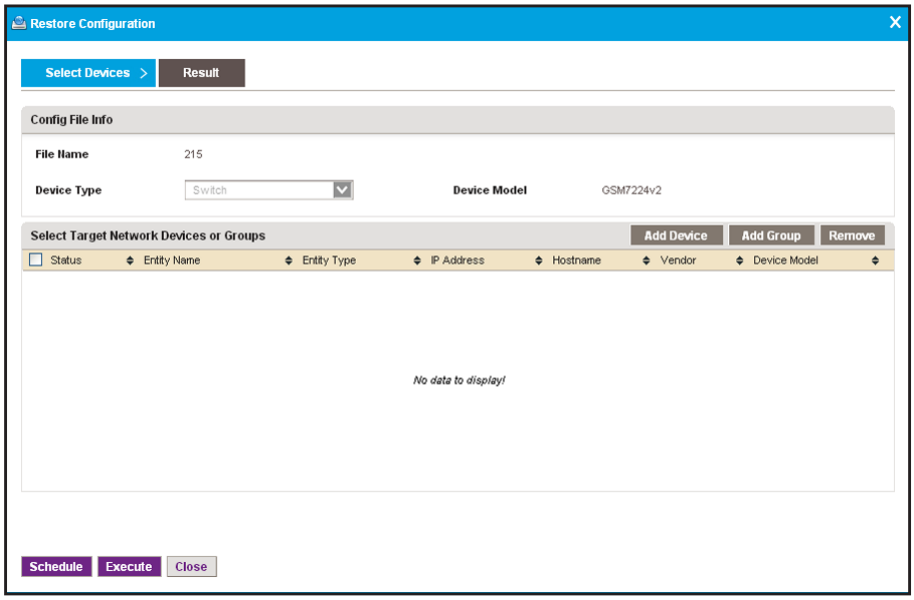
4. To filter the configuration files that are listed, click the **Show Filter** button.

   You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

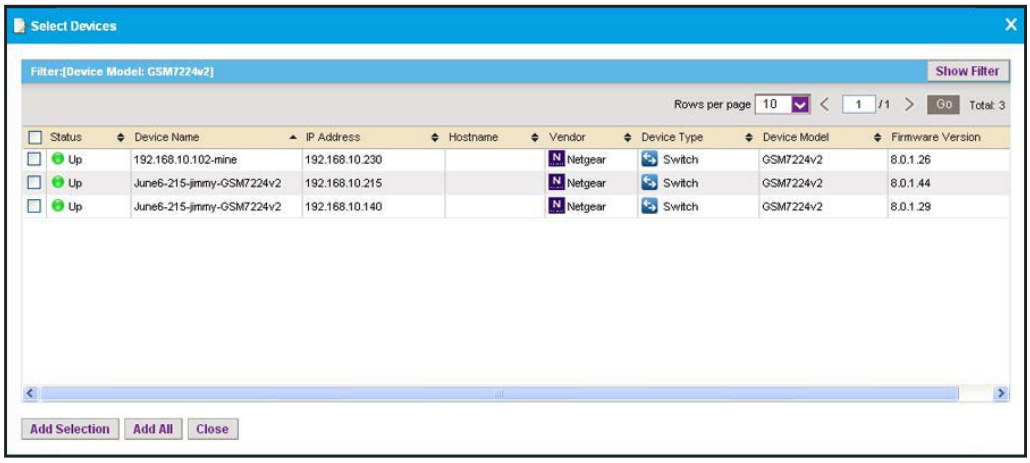
   To hide the filter, click the **Hide Filter** button.

5. Select the configuration file.

6. Click the **Restore Configuration** button.

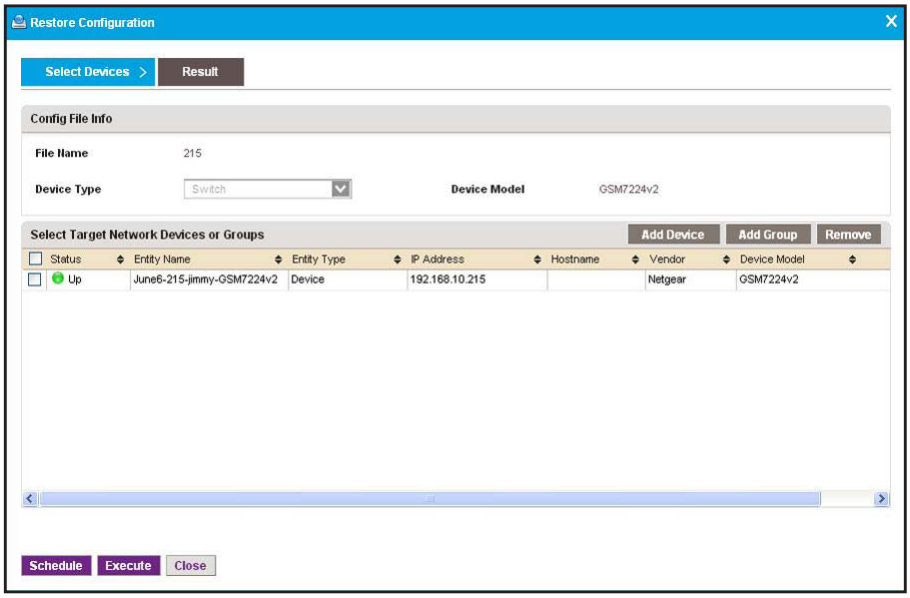


7. Click the **Add Device** button.



8. Select the device.
9. Click the **Add Selection** button.

The screen closes and the selected device is listed on the Restore Configuration screen.

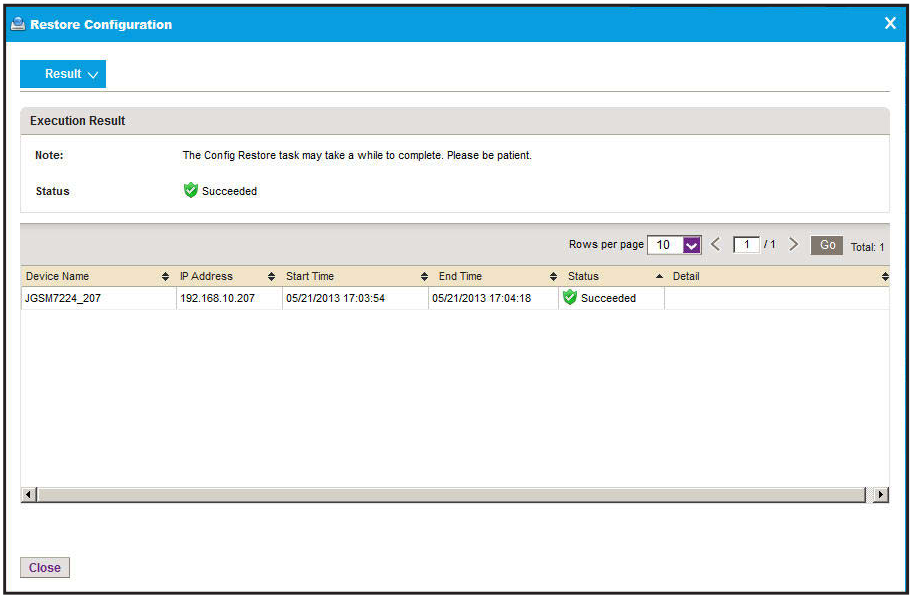


CAUTION:

Make sure that you select the correct device. Selecting the wrong device for the selected configuration file can damage the device.

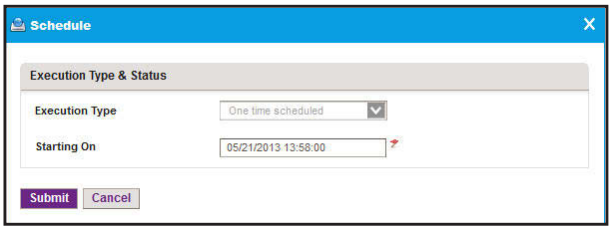
10. Specify whether to restore the configuration file immediately or later by clicking one of the following buttons:
    - **Execute**. Restores the configuration file immediately.

      When the job completes, A screen similar to the following displays.



- **Schedule**. Lets you set up a schedule to restore the configuration file later.

  A screen similar to the following displays.



  a. Specify the time that you want the procedure to start.

  b. Click the **Submit** button.

  The restore procedure is executed once at the specified time.

Customize and Promote a Configuration File

To use the configuration file of a device as a template to configure a collection of devices (see *Restore the Configuration of Several Identical Devices* on page 120), you first must customize the file for your network configuration and promote the file.

Note: For information about using a configuration file as a template to configure several NETGEAR firewalls, see *Promote a Configuration File for Firewalls* on page 117.

CAUTION:

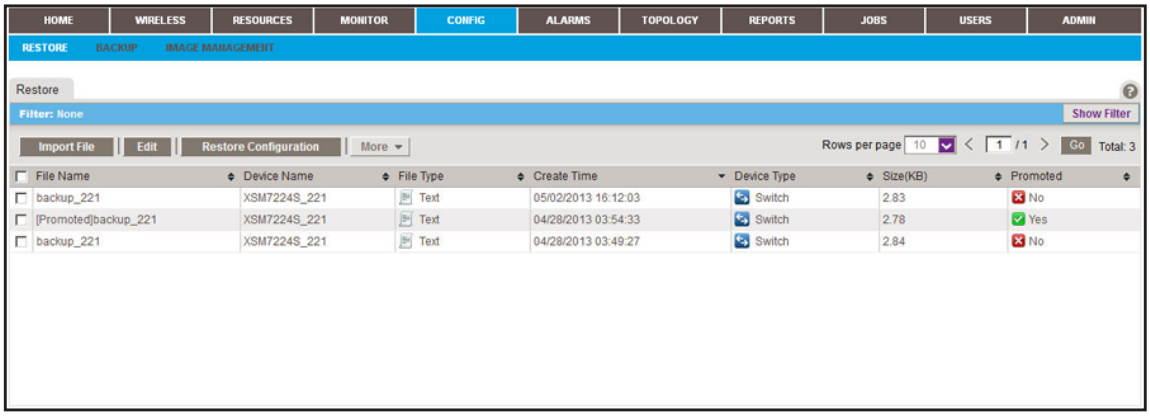
NETGEAR recommends that only administrators with advanced network knowledge and experience perform the following procedure.

➢ **To customize and promote a configuration file:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

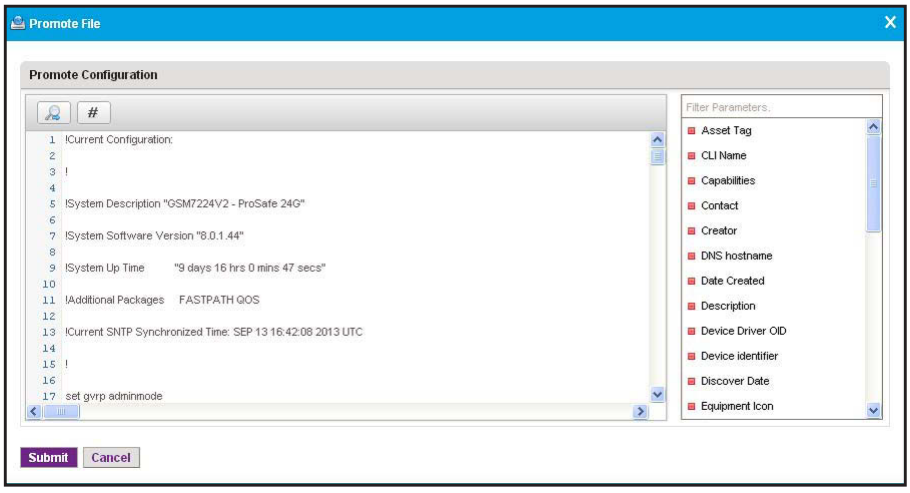
   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

4. To filter the configuration files that are listed, click the **Show Filter** button.

   You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

   To hide the filter, click the **Hide Filter** button.

5. Select the configuration file.
6. From the **More** menu, select **Promote File**.



7. Modify the configuration file by inserting a preconfigured parameter in the configuration file.

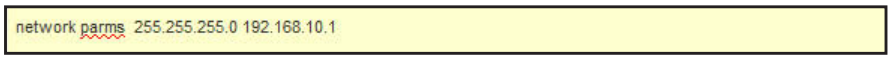
   The application substitutes the parameter that you insert with the actual value that it obtains from the device through monitoring.

a. Select the line of code that you want to modify.

The following figure shows an example of a line of code.

b. Erase the value and leave the cursor positioned where you want the parameter inserted in the line of code.

The following figure shows the example of *Step a* after you erased 192.168.10.202 from the line of code.



c. Double-click a parameter in the Filter Parameters table.

The following figure shows the preconfigured IP Address parameter that you can select from the Filter Parameters table.

The application inserts the parameter at the position of the curser in the line of code.

The following figure shows the example of *Step a* after you inserted the IP Address parameter in the line of code.

8. Repeat *Step 7* until you made all your changes in the configuration file.

CAUTION:

When you restore the configuration of a device, you must provide the correct configuration file. Make sure that any changes that you make on the Promote Configuration screen do not corrupt the configuration file. If you provide a corrupted configuration file, the application pushes out the corrupted configuration file when it executes the configuration restore job and you can damage the device.

9. Click the **Submit** button.

The Promote File screen closes and the promoted configuration file is listed in the Restore table.

Promote a Configuration File for Firewalls

To use the configuration file of a single NETGEAR firewall as a template to configure a collection of NETGEAR firewalls (see *Restore the Configuration of Several Identical Devices* on page 120), you must promote the file but can retain the existing configurations for the following features:

- ISP login and type of ISP
- WAN Internet (IP) address and DNS servers
- Dynamic DNS configuration
- SNMP configuration
- Time Zone

For each of these features, you can decide to either retain the existing configuration on the firewalls or overwrite the configuration for the feature with the one from the promoted file.

CAUTION:

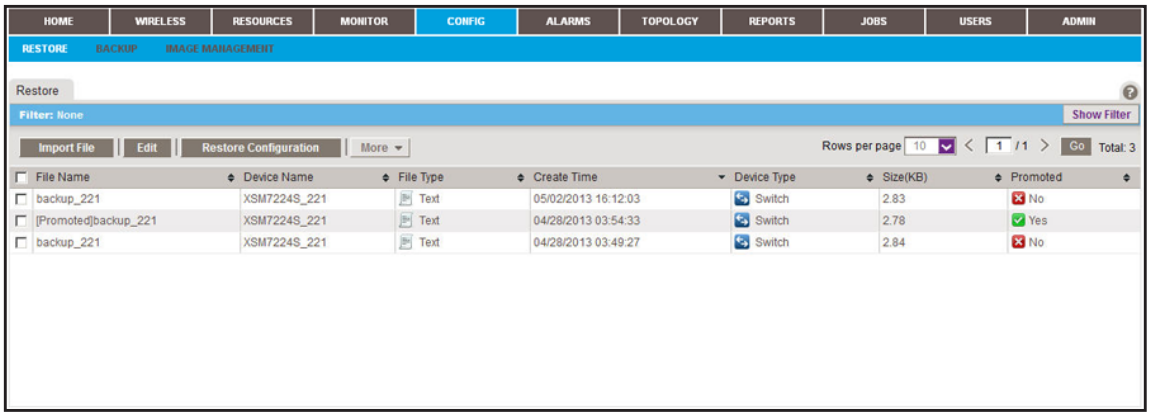
NETGEAR recommends that only administrators with advanced network knowledge and experience perform the following procedure.

➢ **To promote a configuration file for a firewall:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

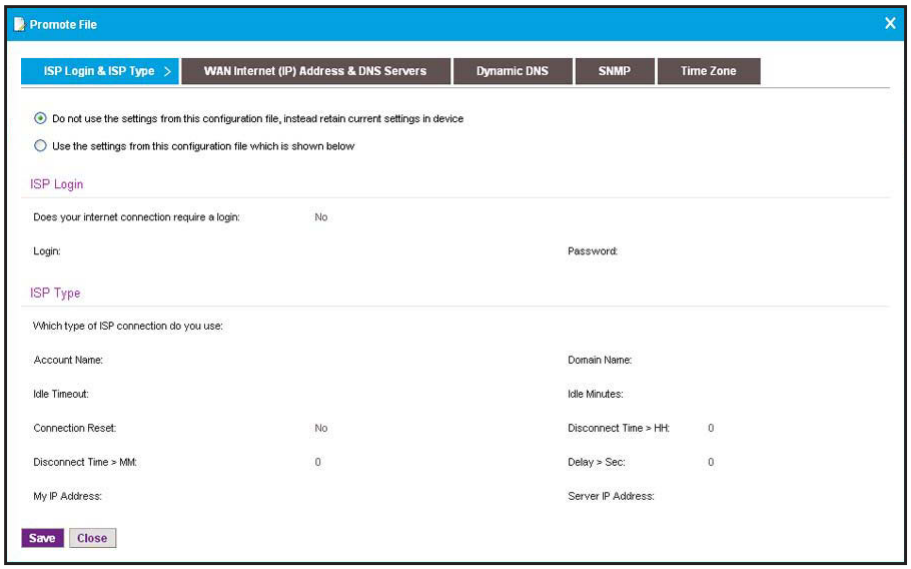
   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

4. To filter the configuration files that are listed, click the **Show Filter** button.

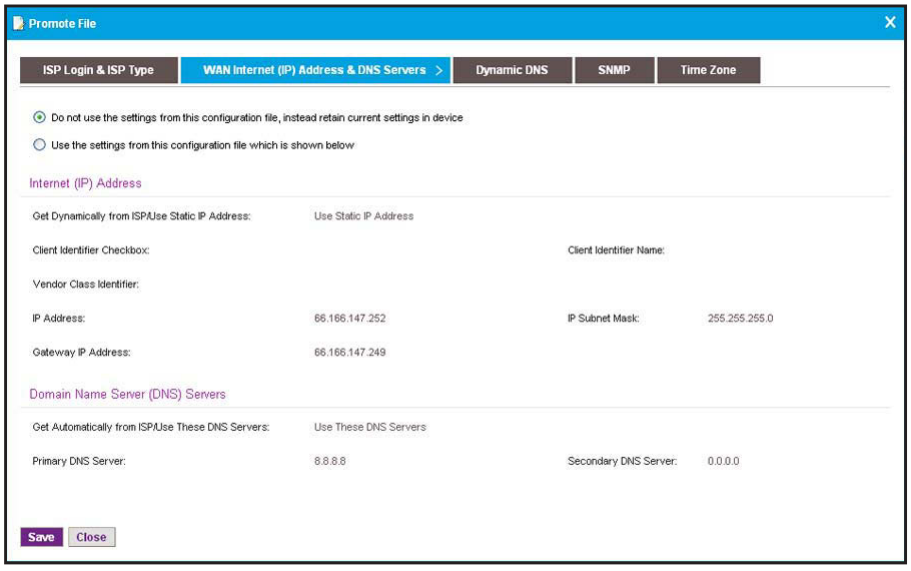
You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

To hide the filter, click the **Hide Filter** button.

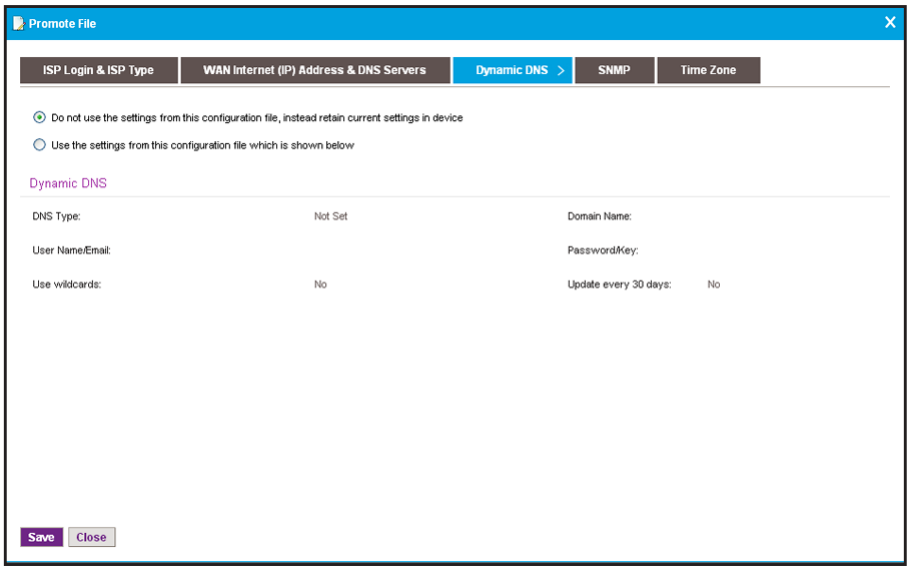
5. Select the configuration file for a firewall, such as the NETGEAR FVS318G firewall.
6. From the **More** menu, select **Promote File**.



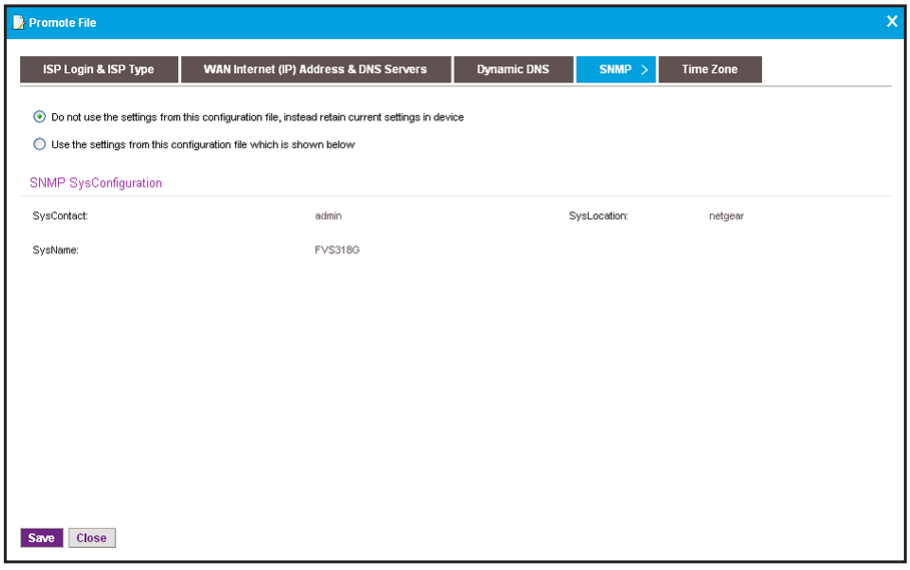
7. Select one of the following radio buttons:
   - **Do not use the settings from this configuration file, instead retain current settings in device**.
   - **Use the settings from this configuration file which is shown below**.
8. Click the **WAN Internet (IP) Address Servers** tab.



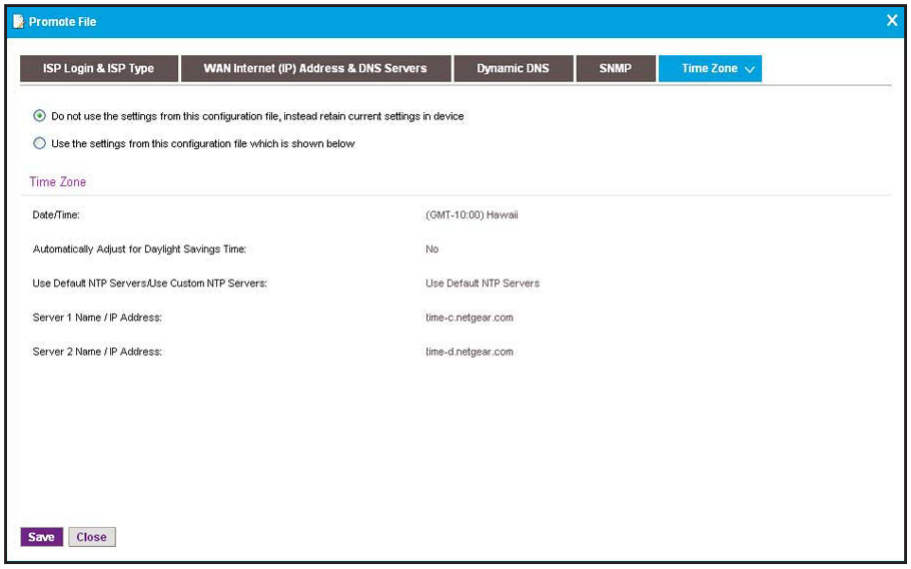
9. Select one of the following radio buttons:
   - **Do not use the settings from this configuration file, instead retain current settings in device**.
   - **Use the settings from this configuration file which is shown below**.
10. Click the **Dynamic DNS** tab.



11. Select one of the following radio buttons:
   - **Do not use the settings from this configuration file, instead retain current settings in device**.
   - **Use the settings from this configuration file which is shown below**.
12. Click the **SNMP** tab.



13. Select one of the following radio buttons:
    - **Do not use the settings from this configuration file, instead retain current settings in device**.
    - **Use the settings from this configuration file which is shown below**.
14. Click the **Time Zone** tab.


Promote File
ISP Login & ISP Type
WAN Internet (IP) Address & DNS Servers
Dynamic DNS
SNMP
Time Zone
Do not use the settings from this configuration file, instead retain current settings in device
Use the settings from this configuration file which is shown below
Time Zone
Date/Time:
(GMT-10:00) Hawaii
Automatically Adjust for Daylight Savings Time:
No
Use Default NTP Servers/Use Custom NTP Servers:
Use Default NTP Servers
Server 1 Name / IP Address:
time-c.netgear.com
Server 2 Name / IP Address:
time-d.netgear.com
Save
Close

CAUTION:

When you restore the configuration of a device, you must provide the correct configuration file. Make sure that you configure the configuration file correctly. If you provide a corrupted configuration file, the application pushes out the corrupted configuration file when it executes the configuration restore job and you can damage the device.

15. Click the **Save** button.

    The Promote File screen closes and the promoted configuration file is listed in the Restore table.

Restore the Configuration of Several Identical Devices

You can use the configuration file of one of the devices on your network to create a template configuration for several identical devices on your network. You must promote this template configuration file before you can use it to restore the configuration of several devices (see *Customize and Promote a Configuration File* on page 114 or *Promote a Configuration File for Firewalls* on page 117). Otherwise, the restore procedure fails.

You can restore the configuration of several devices immediately or schedule the application to restore the configuration later.

CAUTION:

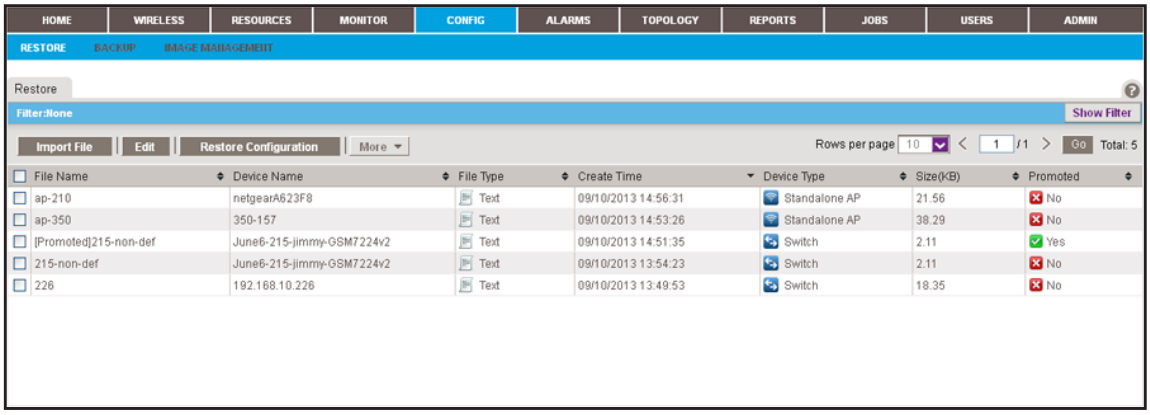
NETGEAR recommends that only administrators with advanced network knowledge and experience perform the following procedure.

➢ **To configure several identical devices:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

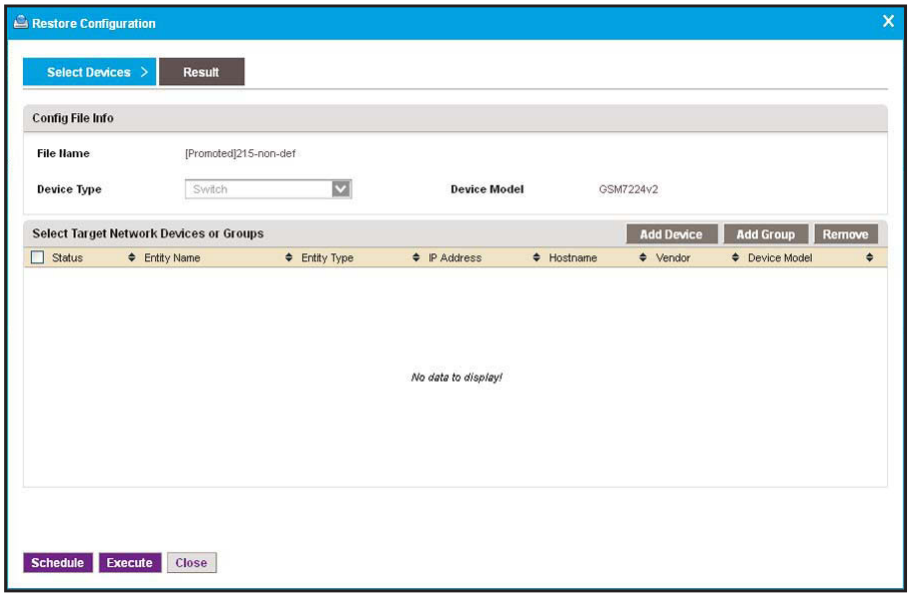
4. To filter the configuration files that are listed, click the **Show Filter** button.

   You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

   To hide the filter, click the **Hide Filter** button.

5. Select the promoted configuration file.

6. Click the **Restore Configuration** button.

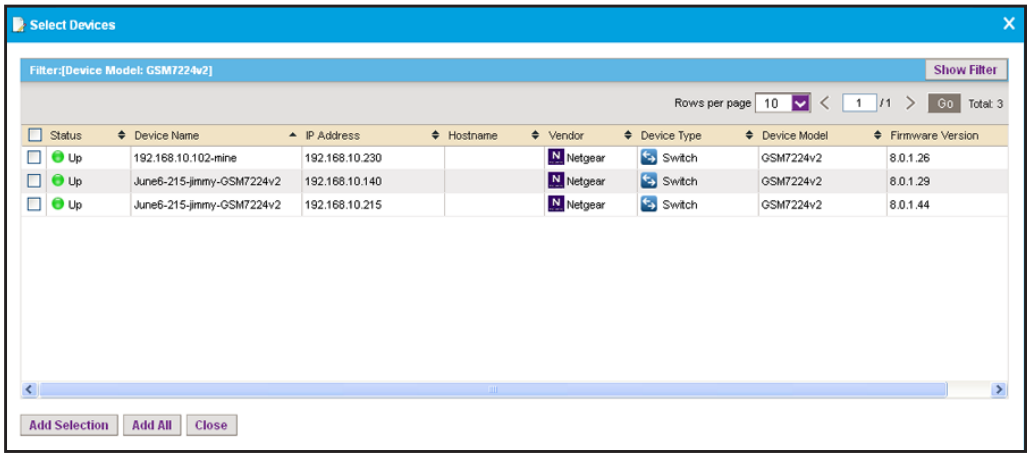


7. Select the target network devices or groups.

CAUTION:

Make sure that you select the correct devices or device groups. Selecting the wrong devices or device groups for the selected configuration file can damage the devices.

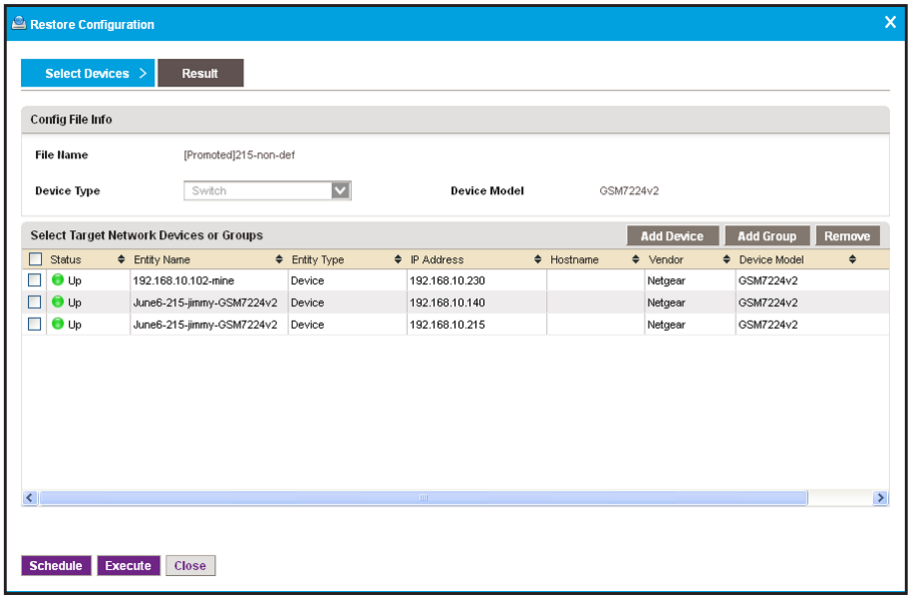
- To add individual devices:
  a. Click the **Add Device** button.



  b. Select the devices you want to add and click the **Add Selection** button.

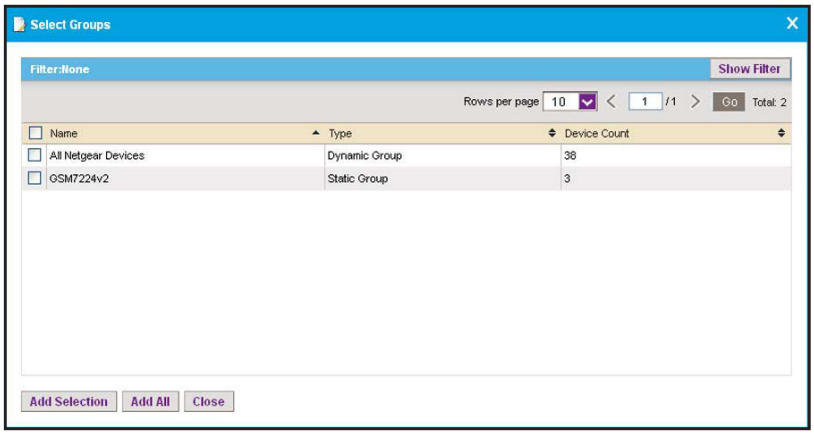
  To add all devices, click the **Add All** button.

The screen closes and the selected devices are listed on the Restore Configuration screen.



- To add device groups:

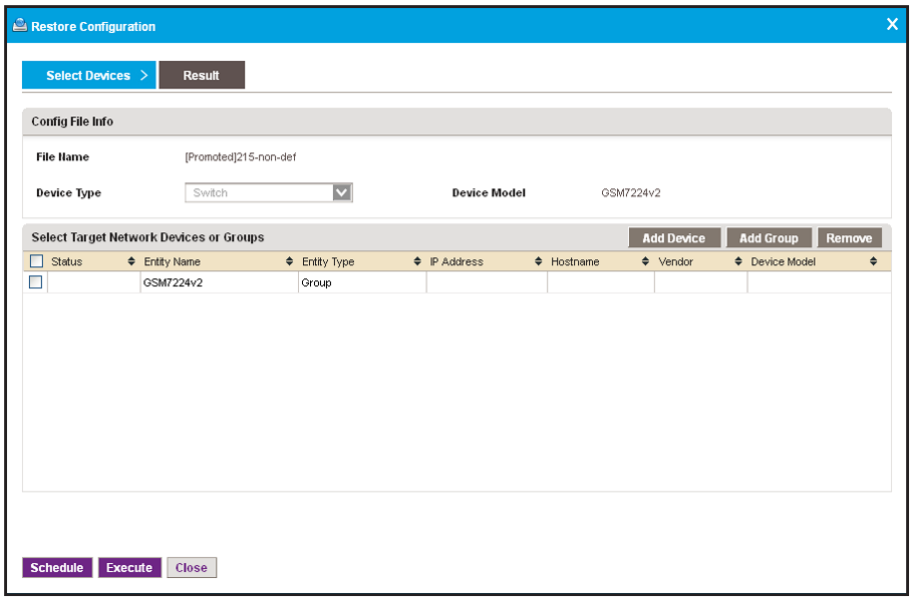
  a. Click the **Add Group** button.



  b. Select the groups you want to add and click the **Add Selection** button.

  To add all groups, click the **Add All** button.

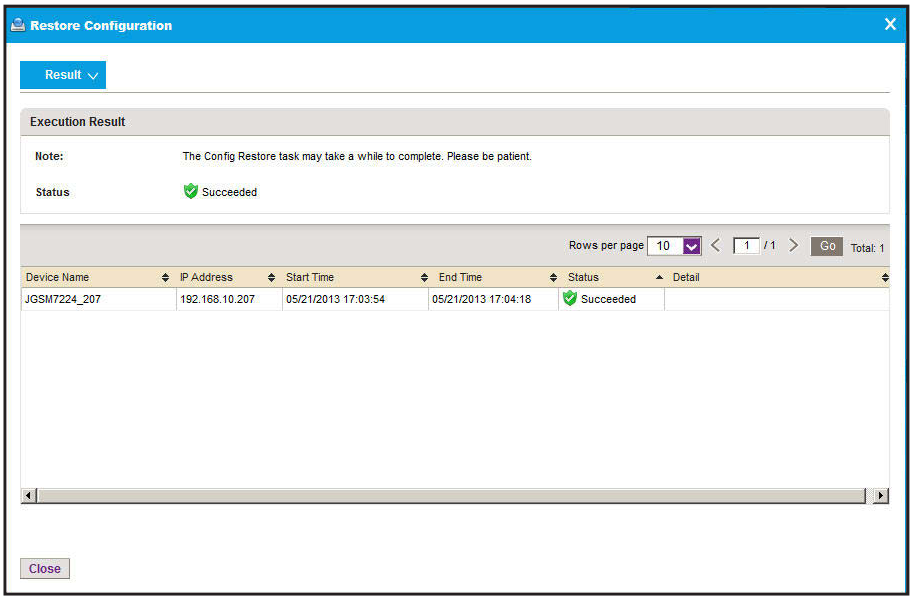
The screen closes and the selected groups are listed on the Restore Configuration screen.



8. Specify whether to restore the configuration file immediately or later by clicking one of the following buttons:

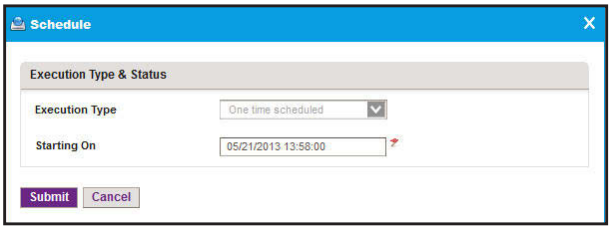
   - **Execute**. Restores the configuration file immediately.

     When the job completes, A screen similar to the following displays.



   - **Schedule**. Lets you set up a schedule to restore the configuration file later.

A screen similar to the following displays.



a. Specify the time that you want the procedure to start.

b. Click the **Submit** button.

The restore procedure is executed once at the specified time.

Import a Configuration File

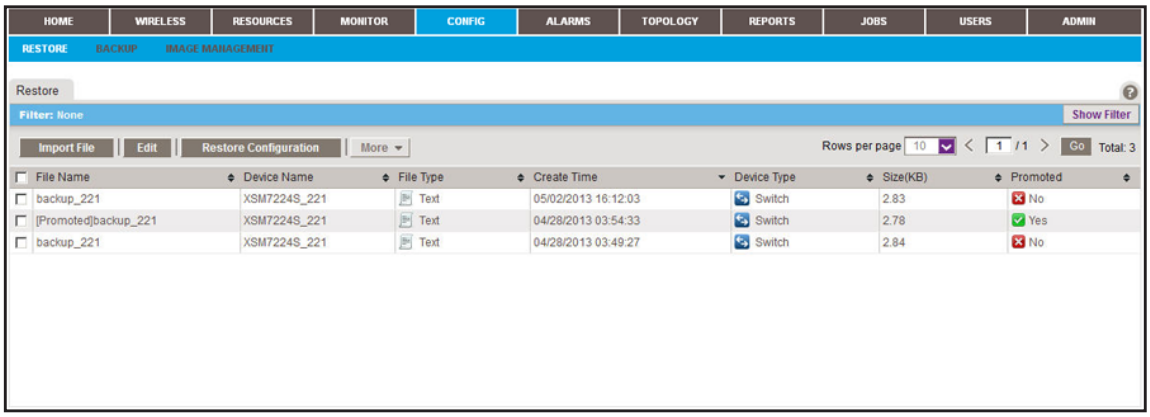
You can import a configuration file for a device. If you want to use an MD5 file for error checking during the import process, first use an MD5 tool to generate an MD5 file that is based on the configuration file that you want to import.

➢ **To import a configuration file for a device:**

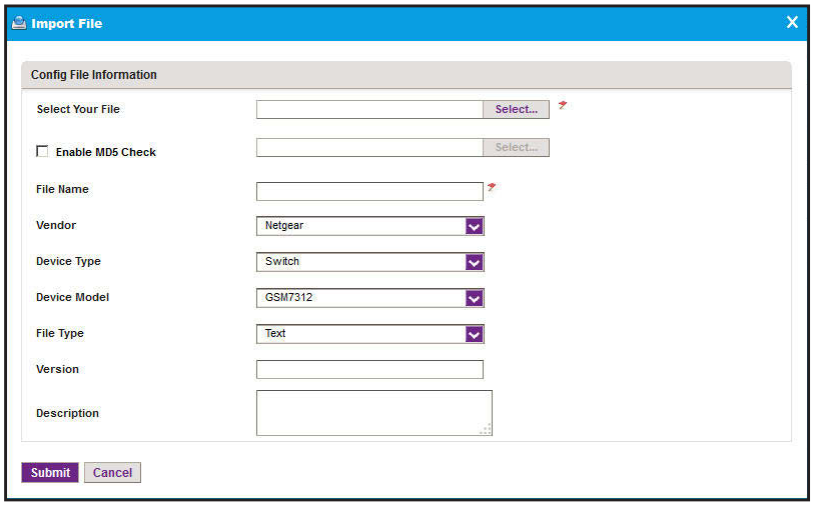
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. Click the **Import File** button.



4. Specify the following information:
   - **Select Your File**. Click the **Select** button.

     Select the image file from your computer, follow the directions of your browser.
   - **Enable MD5 Check**. To enable file validation with the Message Digest 5 algorithm, select this check box and click the **Select** button.

     To select the MD5 file from your computer, follow the directions of your browser.
   - **File Name**. Enter the name of the configuration file that you want to use.
   - **Vendor**. Select the vendor of the device.
   - **Device Type**. Select the device type.
   - **Device Model**. Select the device model.
   - **File Type**. Select the file type.
   - **Version**. Enter the version of the configuration file.
   - **Description**. Enter a description of the configuration file.
5. Click the **Submit** button.

   The Import File screen closes and the imported file is listed in the Restore table.

Export a Configuration File

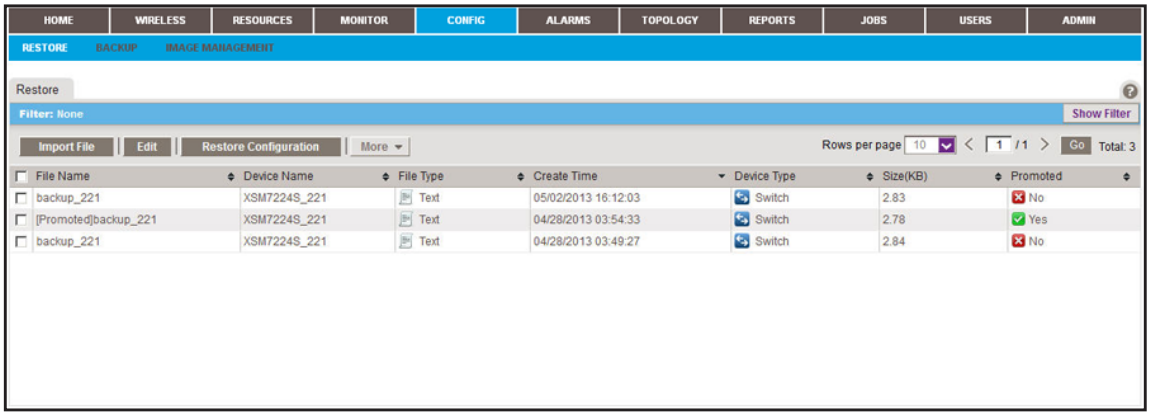
You can export a configuration file for a device.

➢ **To export a configuration file for a device:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

4. To filter the configuration files that are listed, click the **Show Filter** button.

   You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

   To hide the filter, click the **Hide Filter** button.

5. Select the configuration file.
6. From the **More** menu, select **Export File**.
7. To save the file on your computer, follow the directions of your browser.

Modify a Configuration File

You can modify a configuration file except for the configuration file for a NETGEAR firewall. The configuration file of a NETGEAR firewall includes content in hexadecimal format.

CAUTION:

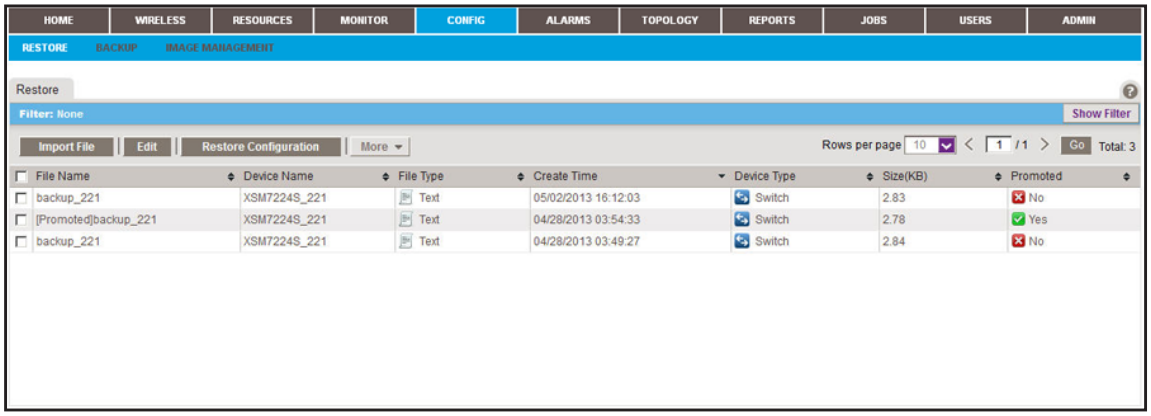
NETGEAR recommends that only administrators with advanced network knowledge and experience perform the following procedure.

➢ **To modify a configuration file:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

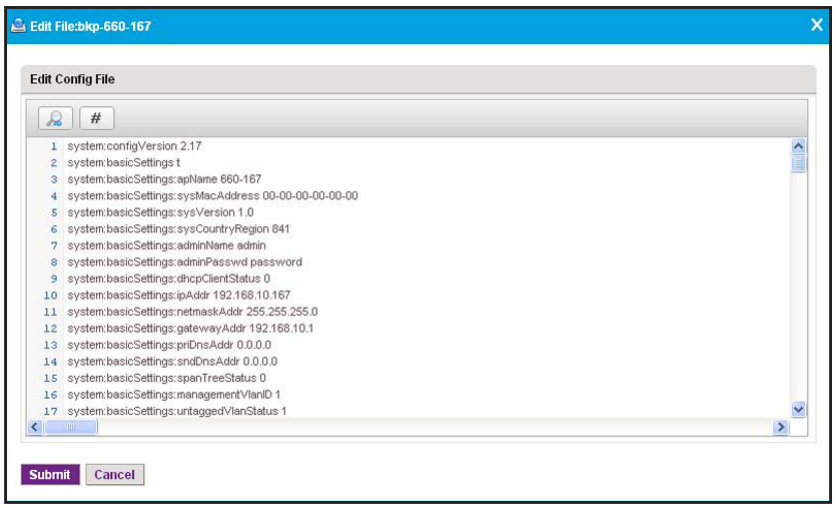
   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

4. To filter the configuration files that are listed, click the **Show Filter** button.

   You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

   To hide the filter, click the **Hide Filter** button.

5. Select the configuration file.
6. Click the **Edit** button.



7. Modify the configuration file by changing, inserting, deleting, or overwriting information.

   The following tools are at your disposal:

   - **Looking glass icon**. Displays the Find/Replace pop-up screen.
   - **Number sign icon**. Displays the Jump to Line pop-up screen.

CAUTION:

When you restore the configuration of a device, you must provide the correct configuration file. Make sure that any changes that you make to the configuration file do not corrupt the file. If you provide a corrupted configuration file, the application pushes out the corrupted configuration file while it executes the configuration restore job and you can damage the device.

8. Click the **Submit** button.

   The modified file is saved and the screen closes.

Remove a Configuration File

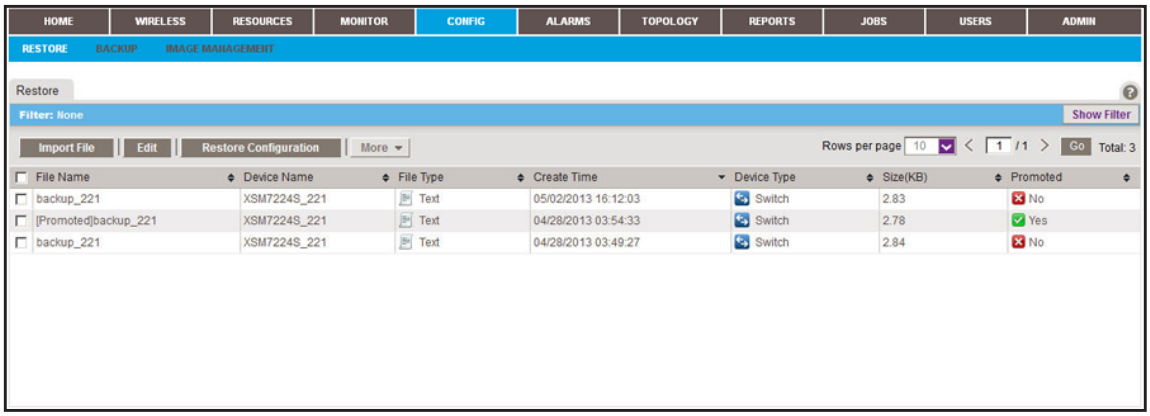
You can remove a configuration file that you no longer need.

➢ **To remove a configuration file:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

4. To filter the configuration files that are listed, click the **Show Filter** button.

   You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

   To hide the filter, click the **Hide Filter** button.

5. Select the configuration file.

6. From the **More** menu, select **Delete File**.

   A pop-up confirmation screen displays.

7. Click the **Yes** button.

   The file is removed from the Restore table and deleted.

Compare Two Configuration Files

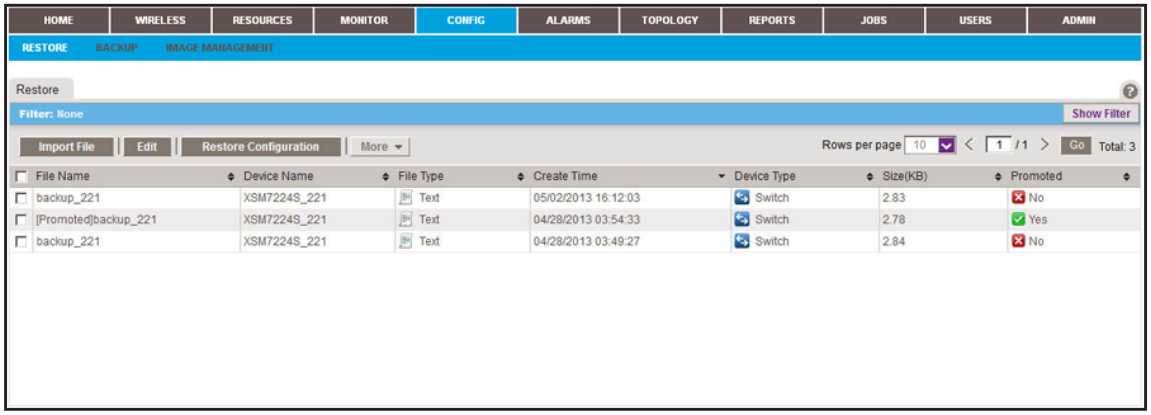
You can compare two configuration files. The files must be text files. You cannot compare binary files.

➢ **To compare two configuration files:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > RESTORE**.



3. To add columns to or remove them from the Restore table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: File Name, Device Name, File Type, Create Time, Device Type, Size (KB), Promoted, Description, Device IP, Device Model, Version, Vendor, and Created By.

4. To filter the configuration files that are listed, click the **Show Filter** button.

   You can filter the configuration files by criteria such as device type, device model, device name, and device IP address.

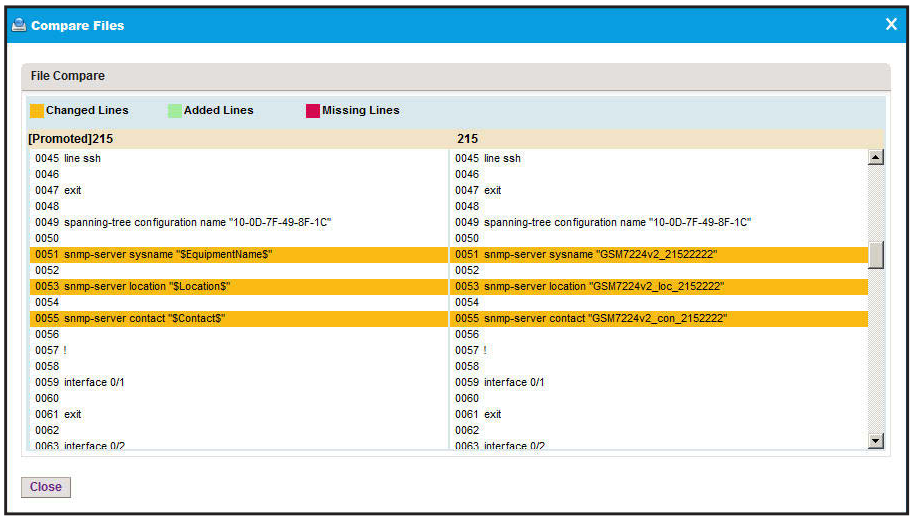
   To hide the filter, click the **Hide Filter** button.

5. Select the two configuration files that you want to compare.

   Both files must be text files.

6. From the **More** menu, select **Compare Files**.

A screen similar to the following one displays.



The left and right side of the screen each display one of the selected files. The screen highlights changed lines in yellow, added lines in green, and missing lines in red.

7. Click the **Close** button.

   The screen closes.

Upgrade Firmware for One or More Devices

NETGEAR posts the latest firmware for each NETGEAR device on *support.netgear.com*. NETGEAR recommends that you visit this site regularly to see if new firmware is available.

CAUTION:

When you update the firmware of a device, you must provide the correct firmware file. Make sure that you select both the correct device type and correct device model for the firmware file that you upload to the application. If you provide the wrong firmware file, the application pushes out the incorrect firmware file while it executes the firmware upgrade and you can damage the device.

CAUTION:

When you update the firmware of stacked switches, make sure that all of the switches in the stack support the firmware that you select to update on the stack master.

The following sections describe the tasks that are related to firmware upgrades:

- *Import a Firmware File*
- *Execute or Schedule a Firmware Upgrade*
- *Modify the File Name, Version Information, and Description for a Firmware File*
- *Export a Firmware File*
- *Remove a Firmware File*

Import a Firmware File

After you download device firmware (an image) from the NETGEAR website at *support.netgear.com* to your computer, you can load the firmware file onto the NMS300 server.

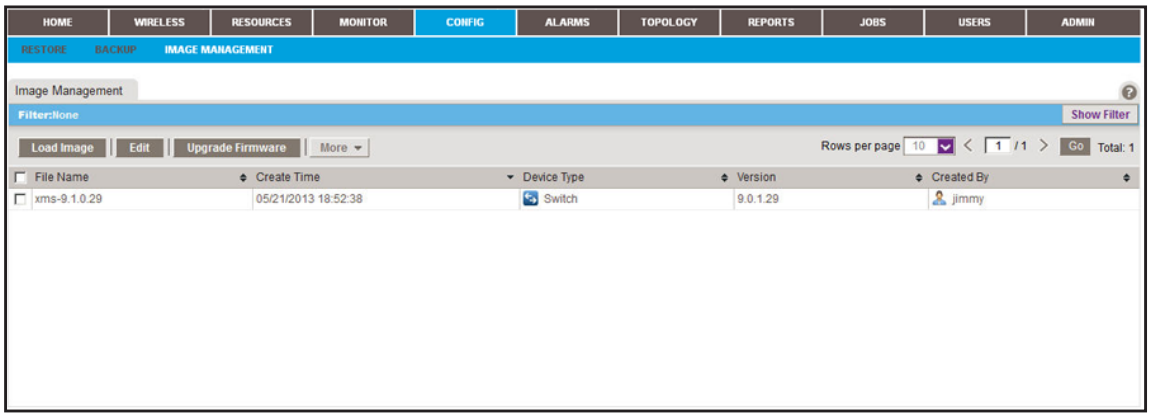
If you want to use an MD5 file for error checking during the import process, first use an MD5 tool to generate an MD5 file that is based on the firmware file that you want to import.

➢ **To load a firmware file onto the NMS300 server:**

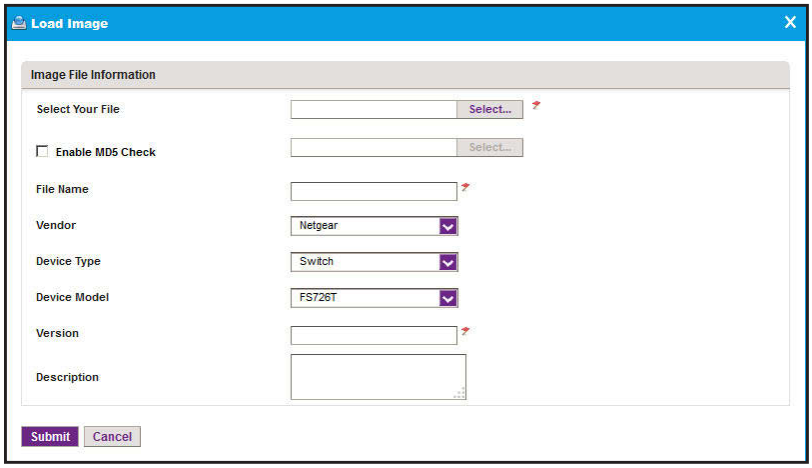
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > IMAGE MANAGEMENT**.



3. Click the **Load Image** button.



4. Specify the following information:
   - **Select Your File**. Click the **Select** button.

     To select the firmware file from your computer, follow the directions of your browser.
   - **Enable MD5 Check**. To enable file validation with the Message Digest 5 algorithm, select this check box and click the **Select** button.

     To select the MD5 file from your computer, follow the directions of your browser.
   - **File Name**. Enter the name of the firmware file.
   - **Vendor**. Select the vendor of the device.
   - **Device Type**. Select the device type.
   - **Device Model**. Select the device model.
   - **Version**. Enter the version of the firmware file.
   - **Description**. Enter a description for the firmware file.
5. Click the **Submit** button.

   The firmware file is transferred from your computer to the NMS300 server.

   The imported firmware file is saved for the data retention period. For more information, see *Set the Data Retention Period* on page 214.

Execute or Schedule a Firmware Upgrade

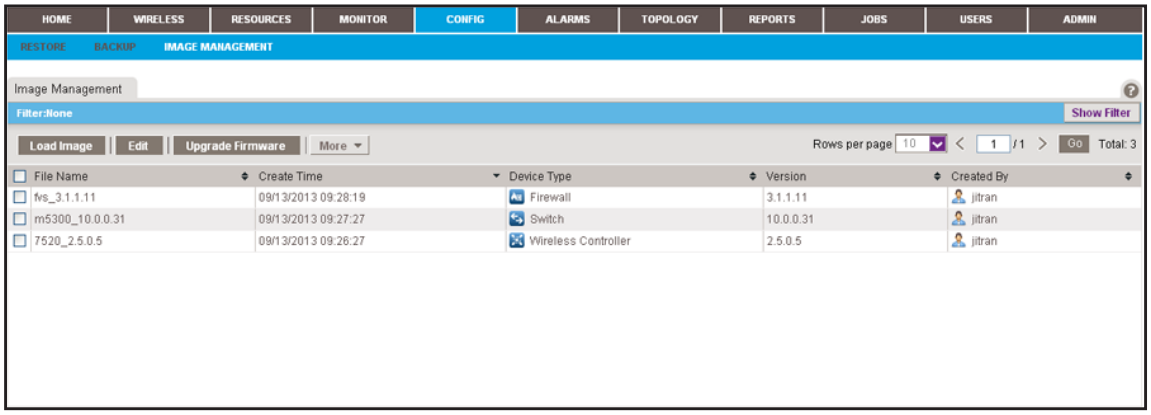
After you import a firmware file into the NMS300 server (see *Import a Firmware File* on page 132), you can execute a firmware upgrade immediately or schedule the application to execute a firmware upgrade later.

➢ **To execute or schedule a firmware upgrade:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > IMAGE MANAGEMENT**.



3. To add columns to or remove them from the Image Management table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

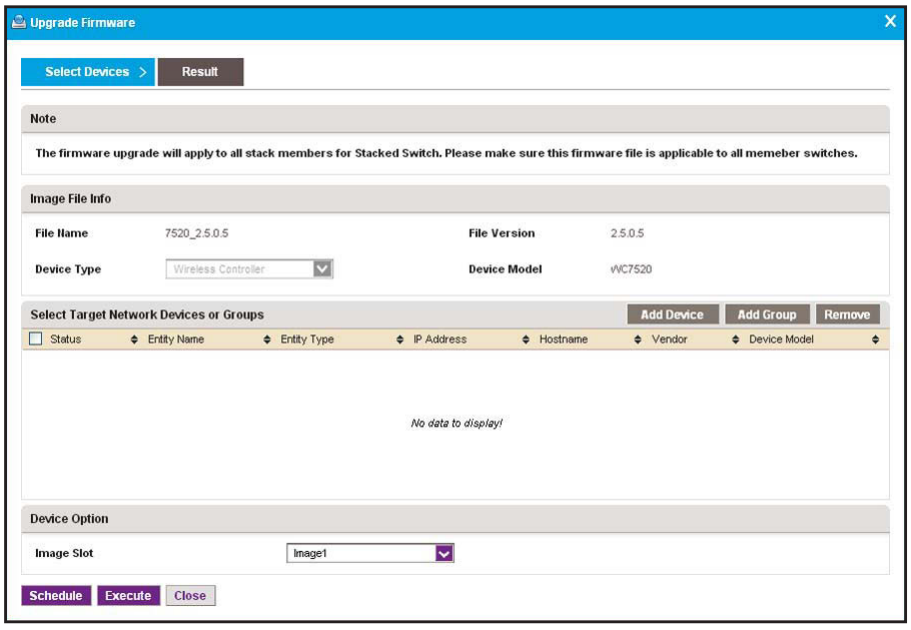
   You can choose from the following columns: File Name, Create Time, Device Type, Version, Created By, Vendor, Device Model, Size (MB), and Description.

4. To filter the firmware files that are listed, click the **Show Filter** button.

   You can filter the firmware files by criteria such as time range, device type, device model, and file name.

   To hide the filter, click the **Hide Filter** button.

5. Select the firmware file.
6. Click the **Upgrade Firmware** button.

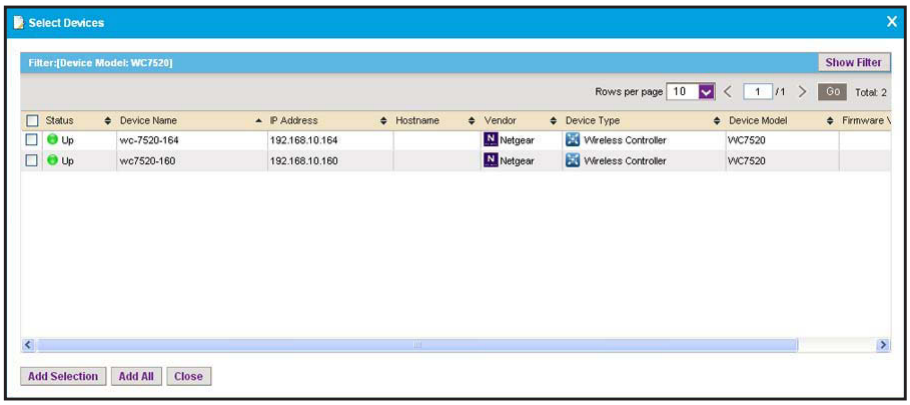


7. Select the target network devices or groups:

CAUTION:

Make sure that you select the correct devices or device groups. Selecting the wrong devices or device groups for the selected firmware file can damage the devices.

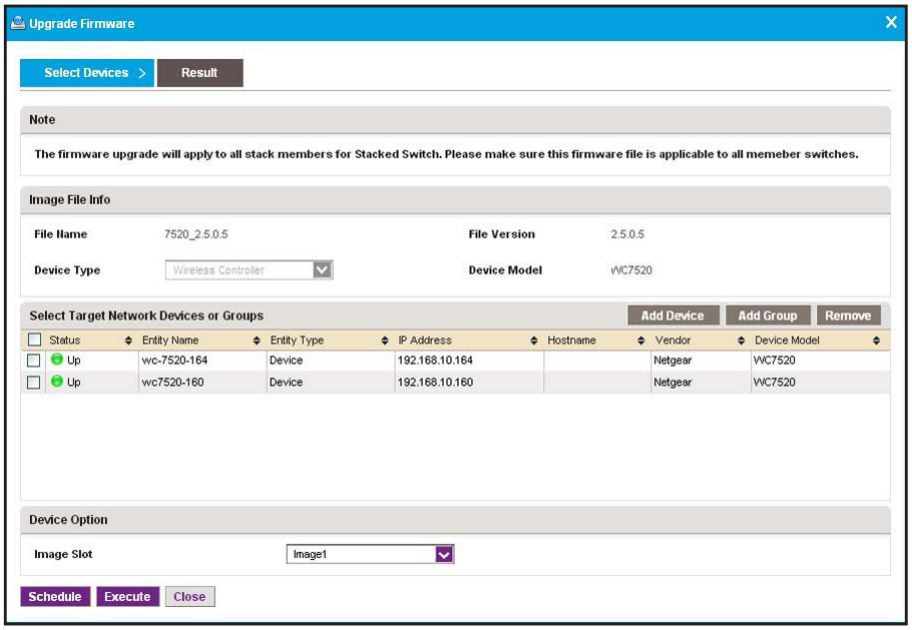
- To specify individual devices:
  a. Click the **Add Device** button.



  b. Select devices and click the **Add Selection** button.

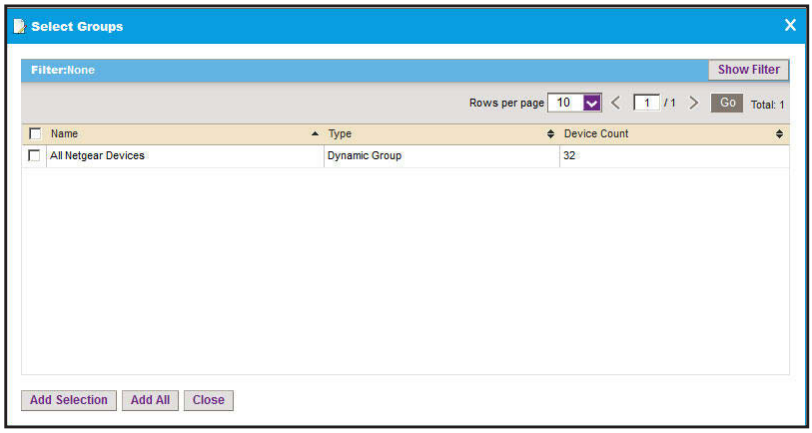
  To add all devices, click the **Add All** button.

  The screen closes and the selected device or devices are listed on the Upgrade Hardware screen.



- To specify device groups:

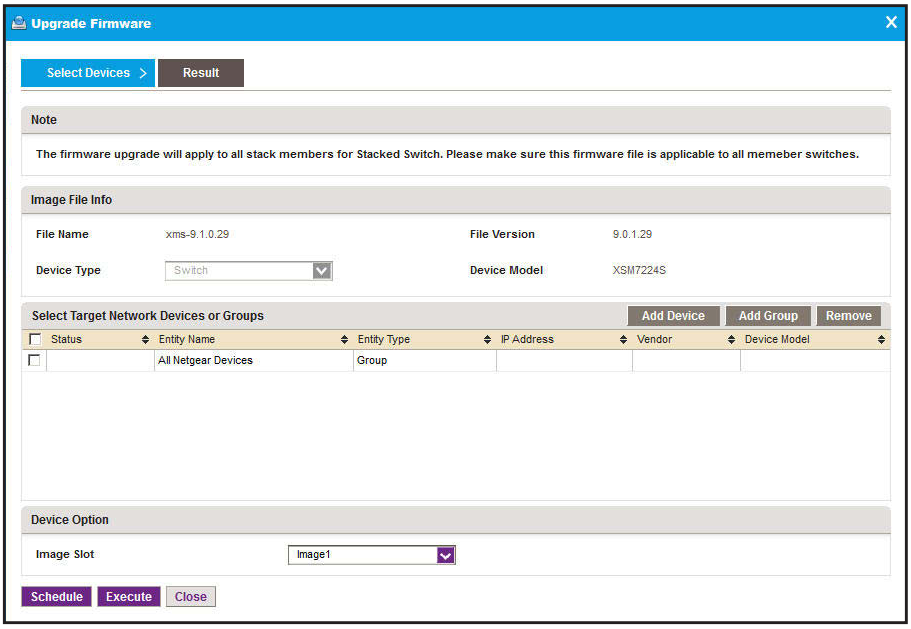
  a. Click the **Add Group** button.



  b. Select groups and click the **Add Selection** button.

  To add all groups, click the **Add All** button.

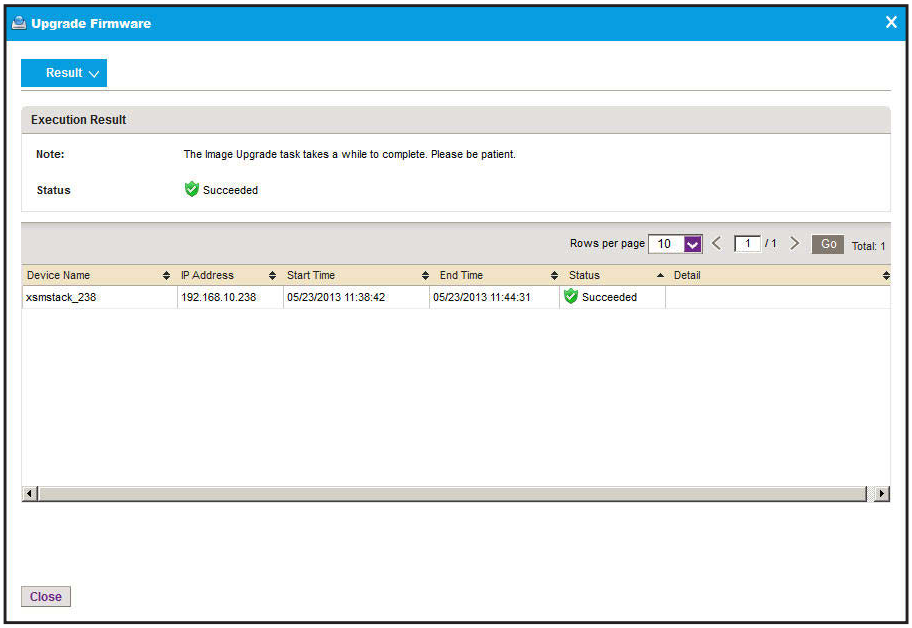
  The screen closes and the selected group or groups are listed on the Upgrade Firmware screen.



8. Specify whether to execute the firmware upgrade immediately or later by clicking one of the following buttons:

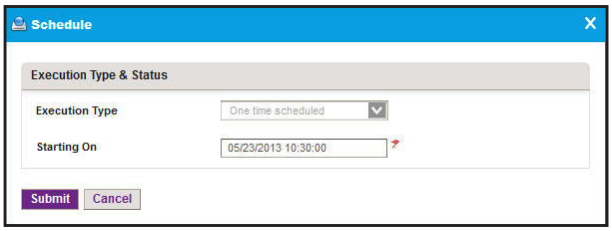
   - **Execute**. Upgrades the firmware immediately.

When the job completes, a Result screen similar to the following displays.



- **Schedule**. Lets you set up a schedule to upgrade the firmware later.

  A screen similar to the following displays.



  a. Specify the time that you want the upgrade to occur.

  b. Click the **Submit** button.

  The upgrade procedure is executed once at the specified time.

Modify the File Name, Version Information, and Description for a Firmware File

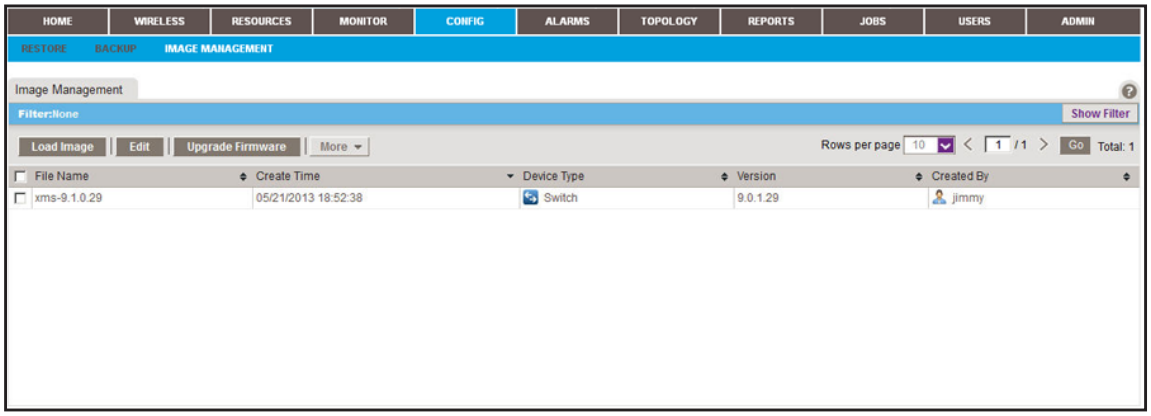
You can modify the file name, version information, and description for a firmware file. You cannot modify the vendor information, device type, and device model for a firmware file.

➢ **To modify information for a firmware file:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > IMAGE MANAGEMENT**.



3. To add columns to or remove them from the Image Management table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

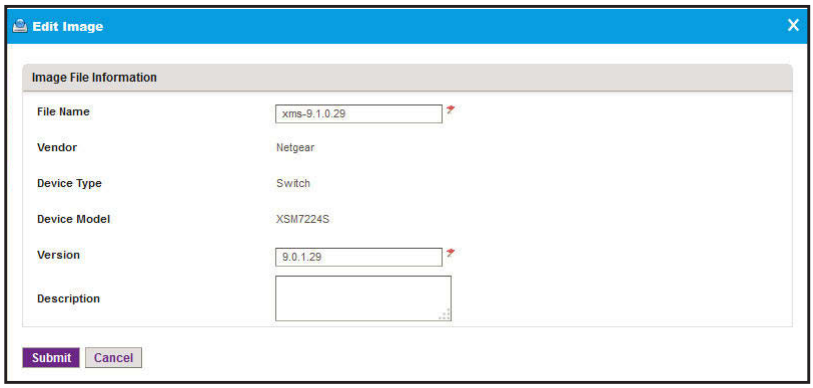
   You can choose from the following columns: File Name, Create Time, Device Type, Version, Created By, Vendor, Device Model, Size (MB), and Description.

4. To filter the firmware files that are listed, click the **Show Filter** button.

   You can filter the firmware files by criteria such as time range, device type, device model, and file name.

   To hide the filter, click the **Hide Filter** button.

5. Select the firmware file.
6. Click the **Edit** button.



7. Modify the information in the **File Name** field, **Version** field, or **Description** field, or in a combination of these fields.
8. Click the **Submit** button.

   The modified firmware file is saved and the screen closes.

Export a Firmware File

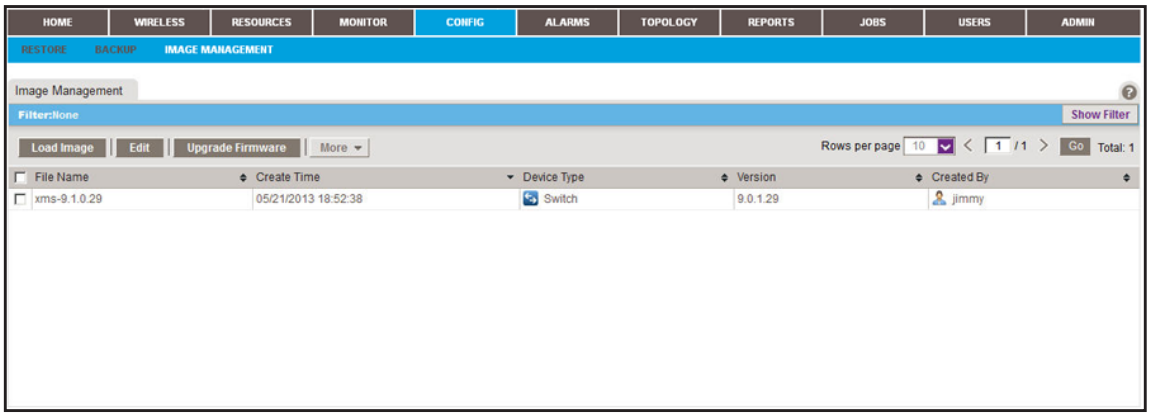
You can export a firmware file.

➢ **To export a firmware file:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > IMAGE MANAGEMENT**.



3. To add columns to or remove them from the Image Management table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: File Name, Create Time, Device Type, Version, Created By, Vendor, Device Model, Size (MB), and Description.

4. To filter the firmware files that are listed, click the **Show Filter** button.

   You can filter the firmware files by criteria such as time range, device type, device model, and file name.

   To hide the filter, click the **Hide Filter** button.

5. Select the firmware file.
6. From the **More** menu, select **Export Image**.
7. To save the firmware file on your computer, follow the directions of your browser.

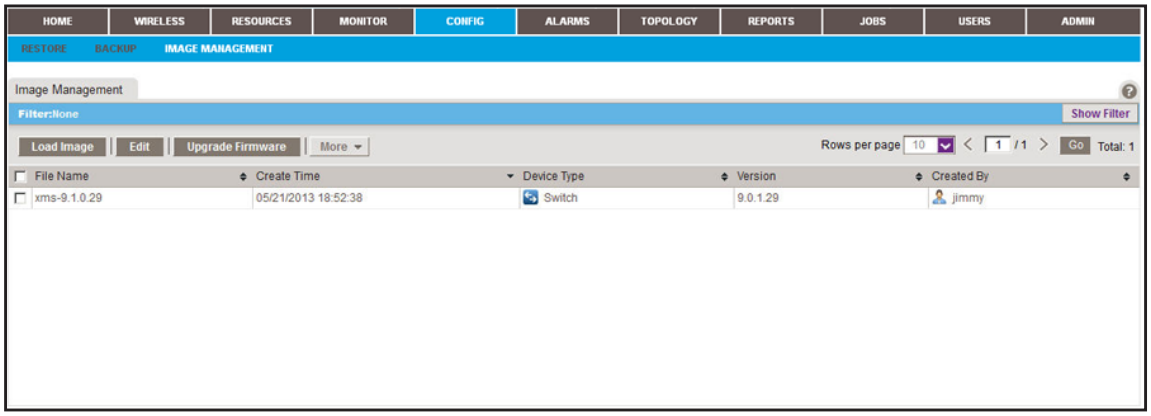
Remove a Firmware File

You can remove a firmware file that you no longer need.

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **CONFIG > IMAGE MANAGEMENT**.



3. To add columns to or remove them from the Image Management table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: File Name, Create Time, Device Type, Version, Created By, Vendor, Device Model, Size (MB), and Description.

4. To filter the firmware files that are listed, click the **Show Filter** button.

   You can filter the firmware files by criteria such as time range, device type, device model, and file name.

   To hide the filter, click the **Hide Filter** button.

5. Select the firmware file.
6. From the **More** menu, select **Delete Image**.

   A pop-up confirmation screen displays.

7. Click the **Yes** button.

   The firmware file is removed from the Image Management table and deleted.

Manage Alarms and Logs

6

Get alerts if something goes wrong

You can receive alarm notifications when conditions are suboptimal and view current and previous alarms using various filter options. As an option, you can receive these alarm notifications by email. In addition, you can view and manage network event notifications, device traps, and device system logs.

This chapter covers the following topics:

- *View and Manage Alarms, Triggers, and Notification Profiles*
- *View and Manage Network Event Notifications*
- *View and Manage Device Traps*
- *View and Manage Device System Logs*

View and Manage Alarms, Triggers, and Notification Profiles

The application provides many default alarms, including status alarms, monitor alarms, and trap alarms. If an upper or lower threshold is exceeded, an alarm configuration generates an alarm.

You can view and manage the current alarms, and you can view and manage the alarm history. You can also add custom alarm configurations that are based on existing configuration monitors.

One or more optional alarm notification profiles let you specify criteria that enable the application to generate and send a notification email message if an alarm occurs.

The application provides the following four severity levels for alarms:

- Critical (by default, red color indication)
- Major (by default, yellow color indication)
- Minor (by default, blue color indication)
- Info (by default, no color indication)

The following sections describe the alarm-related tasks:

- *View and Manage Current Alarms*
- *View and Manage the Alarm History*
- *View and Manage Alarm Configurations*
- *Add a Custom Alarm Configuration*
- *Modify an Alarm Configuration*
- *View and Manage Alarm Notification Profiles*
- *Add or Modify an Alarm Notification Profile*
- *Customize Alarm Colors*

View and Manage Current Alarms

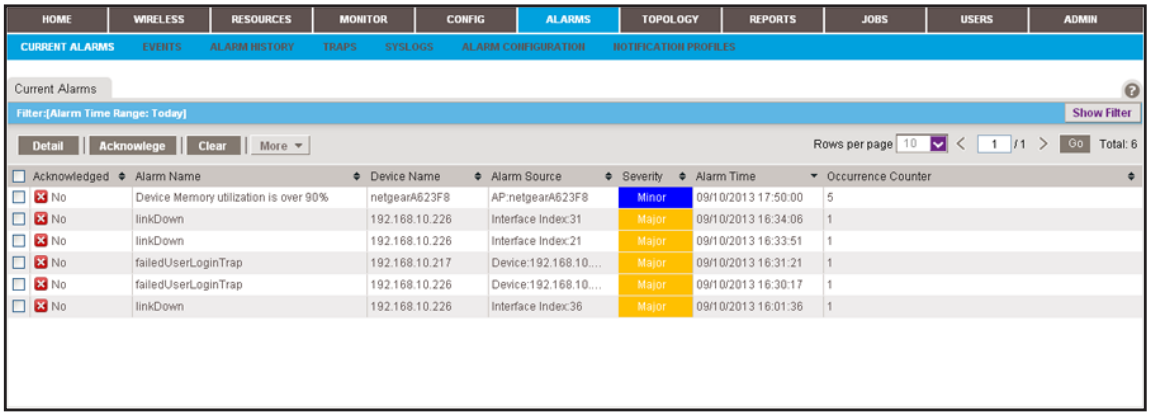
The Current Alarms table shows the active alarms for the entire network. You can acknowledge alarms, display details about alarms, clear alarms, and export alarms.

➢ **To view and manage the current alarms:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > CURRENT ALARMS**.



3. To add columns to or remove them from the Current Alarms table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Acknowledged, Alarm Name, Device Name, Alarm Source, Severity, Alarm Time, Occurrence Counter, Alarm Type, Device IP, Acknowledge By, Acknowledge Time, and Notification OID.

4. To filter the alarm entries that are listed, click the **Show Filter** button.

   You can filter the alarm entries by criteria such as time range, device IP address, and severity level. By default, the alarm entries are filtered to display today's entries.

   To hide the filter, click the **Hide Filter** button.

5. Take one of the following actions:
   - View details for an alarm:
     a. Select the alarm.
     b. Click the **Detail** button.

     c. To close the Alarm Detail screen, click the **Close** button.
   - Acknowledge an alarm:
     a. Select the alarm.
     b. Click the **Acknowledge** button.

        Acknowledging an alarm means that you take ownership of the issue.

- Clear an alarm:
  a. Select the alarm.
  b. Click the **Clear** button.

     Clearing an alarm means that the fault that the alarm indicates no longer exists.
- Acknowledge a batch of alarms:
  a. Select multiple alarms.
  b. From the **More** menu, select **Batch Acknowledge**.
- Clear a batch of alarms:
  a. Select multiple alarms.
  b. From the **More** menu, select **Batch Clear**.
- Export the entire Current Alarms table to an Excel spreadsheet:
  a. From the **More** menu, select **Export to Excel**.
  b. To save the alarms on your computer, follow the directions of your browser.
- Export the entire Current Alarms table to a PDF:
  a. From the **More** menu, select **Export to PDF**.
  b. To save the alarms on your computer, follow the directions of your browser.

View and Manage the Alarm History

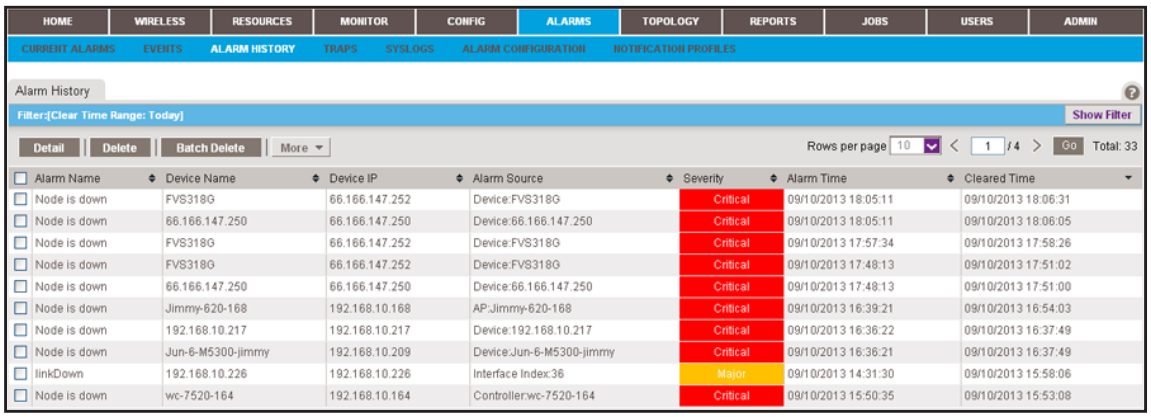
The Alarm History table shows the previous alarms for the entire network. You can remove alarms from this table to reduce the amount of disk space that the application requires on the server. You can also export alarms.

➢ **To view and manage the alarm history:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > ALARM HISTORY**.



3. To add columns to or remove them from the Alarm History table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

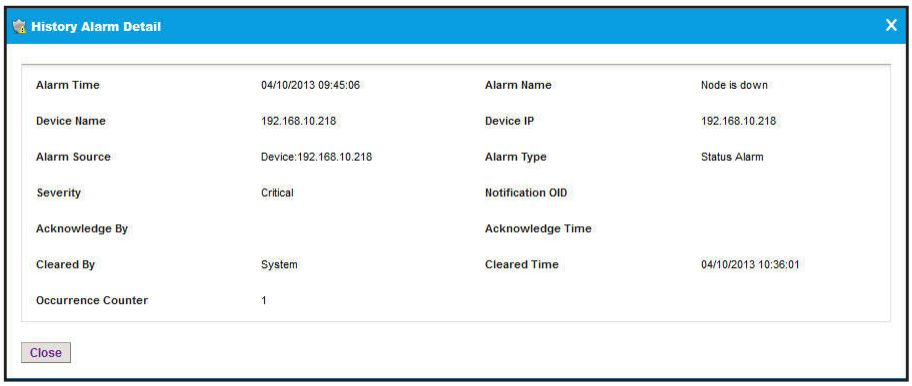
You can choose from the following columns: Alarm Name, Device Name, Device IP, Alarm Source, Severity, Alarm Time, Cleared Time, Notification OID, Cleared By, Alarm Type, and Occurrence Counter.

4. To filter the alarm history entries that are listed, click the **Show Filter** button.

   You can filter the alarm history entries by criteria such as time range, device IP address, and severity level. By default, the alarm history entries are filtered to display today's entries.

   To hide the filter, click the **Hide Filter** button.

5. Take one of the following actions:
   - View details for an alarm:
     a. Select the alarm.
     b. Click the **Detail** button.



     To close the History Alarm Detail screen, click the **Close** button.

   - Delete an alarm:
     a. Select the alarm.
     b. Click the **Delete** button.

        The alarm is removed from the database.

   - Delete a batch of alarms:
     a. Select multiple alarms.
     b. Click the **Batch Delete** button.

        The alarms are removed from the database.

   - Export the entire Alarm History table to an Excel spreadsheet:
     a. From the **More** menu, select **Export to Excel**.
     b. To save the alarms on your computer, follow the directions of your browser.
   - Export the entire Alarm History table to a PDF:
     a. From the **More** menu, select **Export to PDF**.
     b. To save the alarms on your computer, follow the directions of your browser.

View and Manage Alarm Configurations

If an upper or lower threshold is exceeded, an alarm configuration generates an alarm. The application provides many default alarms, including status alarms, monitor alarms, and trap alarms.

The default status alarms include the following critical alarms:

- FTP service is down
- Node is down
- Performance management (PM) collection service error
- Syslog service is down
- TFTP service is down
- Trap service is down

The default monitor alarms include alarms for memory and CPU utilization of devices and disk, CPU, and memory utilization of the NMS300 server. The application provides multiple default trap alarms.

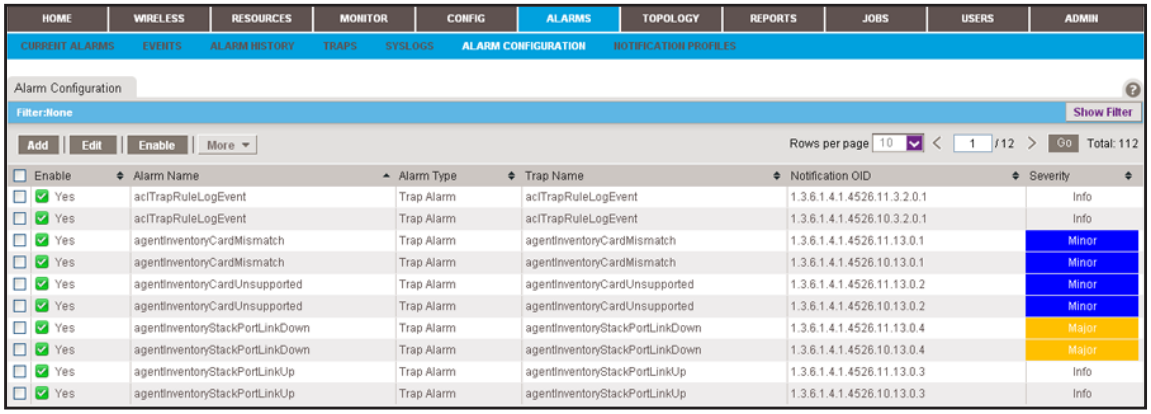
You can view, disable, reenable, remove, and export alarm configurations. For information about how to add a custom alarm configuration, see *Add a Custom Alarm Configuration* on page 148. For information about how to modify an existing alarm configuration, see *Modify an Alarm Configuration* on page 150.

➢ **To view and manage the alarms configurations:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > ALARM CONFIGUATION**.



3. To add columns to or remove them from the Alarm Configuration table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Enable, Alarm Name, Alarm Type, Trap Name, Notification OID, Severity, MIB Name, and Description.

4. To filter the alarm configurations that are listed, click the **Show Filter** button.

You can filter the alarm configuration by criteria such as alarm name, enabled status, alarm type, and severity.

To hide the filter, click the **Hide Filter** button.

5. Take one of the following actions:
   - Disable an alarm configuration:
     a. Select the alarm configuration.
     b. From the **More** menu, select **Disable**.

        A pop-up confirmation screen displays.

     c. Click the **Yes** button.

        The alarm configuration is disabled and can no longer generate an alarm. In the Alarm Configuration table, the Enable column displays No for the alarm configuration.
   - Enable an alarm configuration:
     a. Select the alarm configuration.
     b. Select the **Enable** button.

        The alarm configuration is enabled and can generate an alarm. In the Alarm Configuration table, the Enable column displays Yes for the alarm configuration.
   - Remove an alarm configuration:
     a. Select the alarm configuration.
     b. From the **More** menu, select **Delete**.

        A pop-up confirmation screen displays.

     c. Click the **Yes** button.

        The alarm configuration is removed from the Alarm Configuration table and deleted.
   - Export the entire Alarm Configuration table to an Excel spreadsheet:
     a. From the **More** menu, select **Export to Excel**.
     b. To save the alarm configurations on your computer, follow the directions of your browser.
   - Export the entire Alarm Configuration table to a PDF:
     a. From the **More** menu, select **Export to PDF**.
     b. To save the alarm configurations on your computer, follow the directions of your browser.

Add a Custom Alarm Configuration

You can define your own alarms, including alarms for all configuration monitors (see *Manage the Configuration Monitors* on page 83).

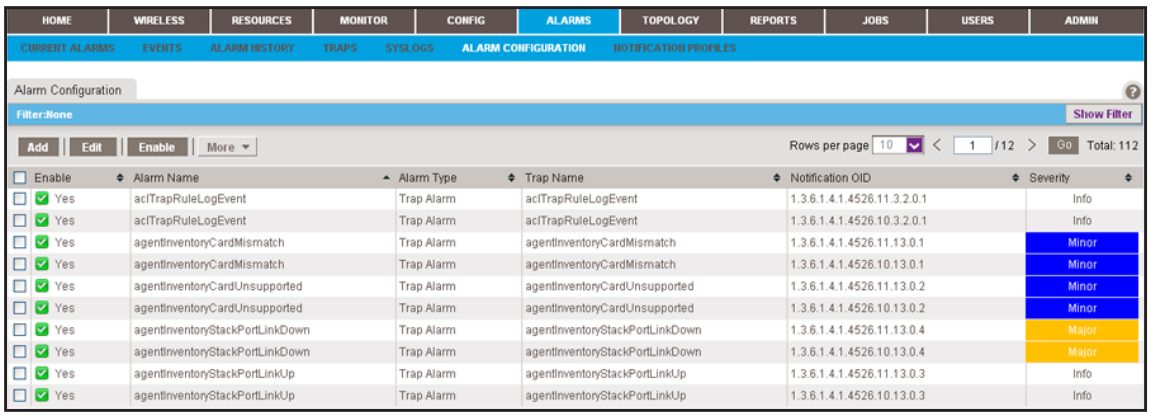
A custom alarm configuration that you add is always based on an existing configuration monitor and includes a threshold. The configuration monitor determines the polling interval for the alarm configuration. For more information, see *Manage the Configuration Monitors* on page 83.

➢ **To add one or more custom alarm configurations:**

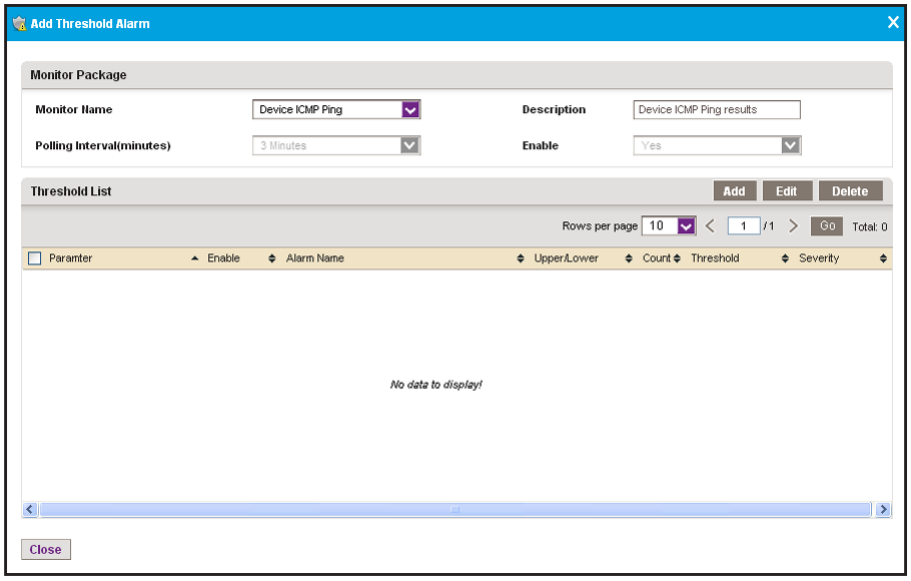
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > ALARM CONFIGUATION**.



3. Click the **Add** button.

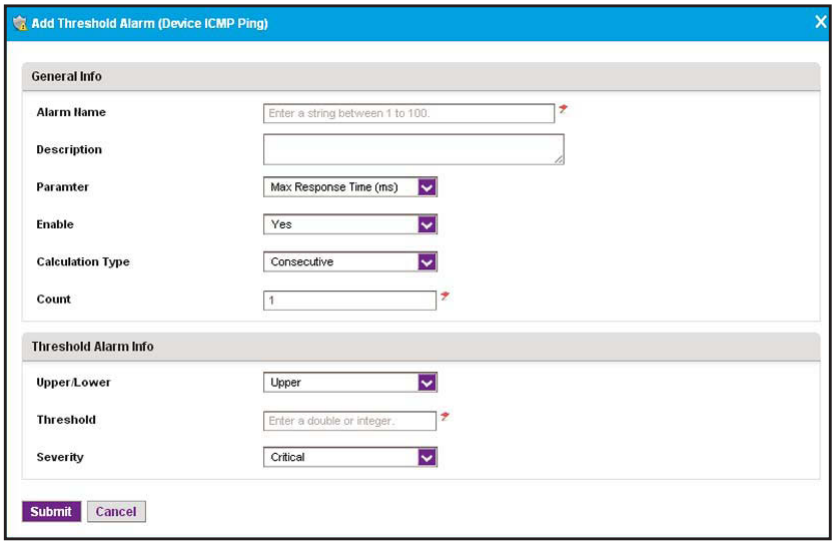


4. From the **Monitor Name** menu, select the monitor.
5. In the **Description** field, enter a new description, or use the default description.

The configuration monitor determines the polling interval for the alarm configuration. For more information, see *Manage the Configuration Monitors* on page 83.

The **Enable** field shows whether the configuration monitor is enabled. However, you can enable an alarm configuration even if the configuration monitor is disabled.

6. Click the **Add** button.



7. Enter the following threshold information:
   - **General Info**:
     - **Alarm Name**. Enter a name for the alarm.
     - **Description**. Enter a description for the alarm.
     - **Parameter**. Select a parameter. The parameters that are displayed in the menu depend on the monitor that you select in *Step 4*.
     - **Enable**. Select whether to enable the threshold.
     - **Calculation Type**. Select a consecutive or average calculation.
     - **Count**. Select the number of times that a particular event must occur before the threshold is met.
   - **Threshold Alarm Info**:
     - **Upper/Lower**. Select an upper or lower threshold.
     - **Threshold**. Enter the threshold. If this threshold is exceeded, the application triggers an alarm.
     - **Severity**. Select whether the alarm is considered critical, major, minor, or informational.
8. Click the **Submit** button.

   The Add Threshold screen for the selected monitor screen closes and the alarm configuration is added to the Threshold List table.
9. To add another alarm configuration, repeat *Step 6* through *Step 8*.

Before you add a new alarm configuration to the Alarm Configuration table, you can still modify or remove the alarm configuration.

10. To close the general Add Threshold screen, click the **Close** button.

    All new alarm configurations are added to the Alarm Configuration table.

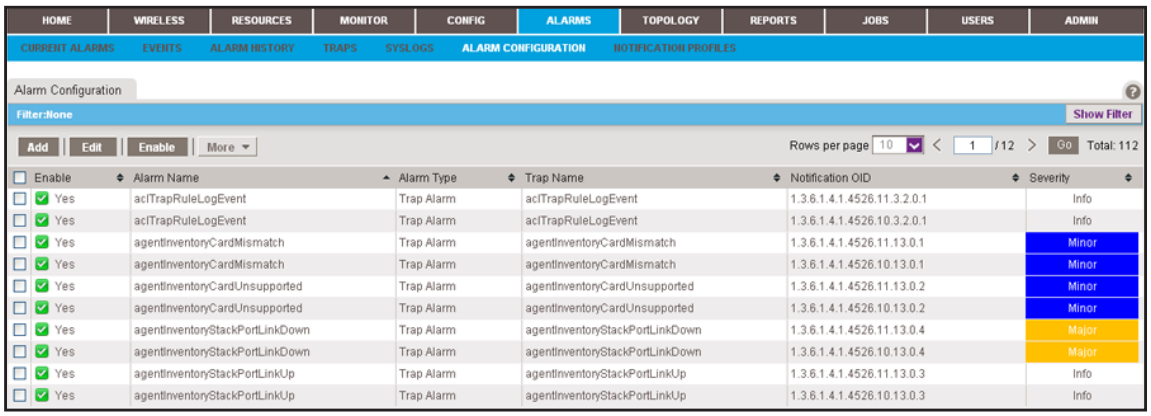
Modify an Alarm Configuration

You can modify a default or custom alarm configuration.

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > ALARM CONFIGUATION**.



3. To add columns to or remove them from the Alarm Configuration table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Enable, Alarm Name, Alarm Type, Trap Name, Notification OID, Severity, MIB Name, and Description.

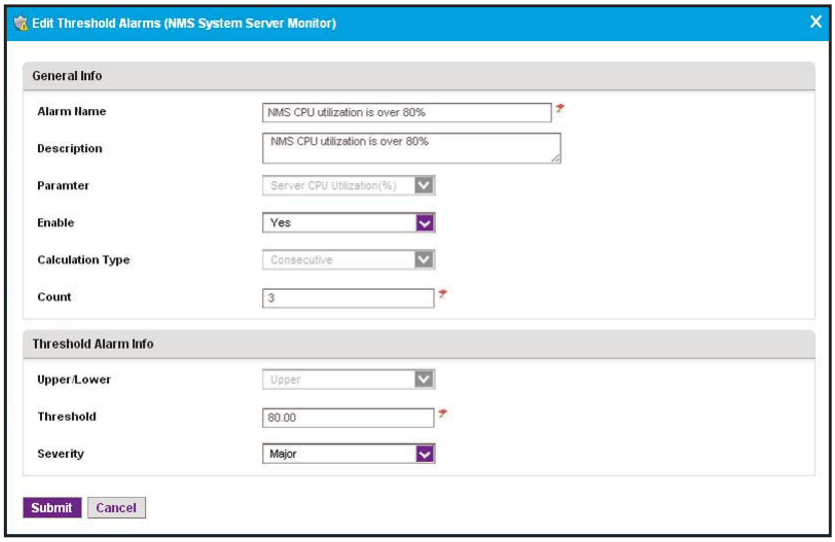
4. To filter the alarm configurations that are listed, click the **Show Filter** button.

   You can filter the alarm configuration by criteria such as alarm name, enabled status, alarm type, and severity.

   To hide the filter, click the **Hide Filter** button.

5. Select the alarm configuration.

6. Click the **Edit** button.



7. Modify the following threshold information as needed:
   - **General Info**:
     - **Alarm Name**. Modify the name for the alarm.
     - **Description**. Modify the description for the alarm.
     - **Parameter**. You cannot modify the parameter.
     - **Enable**. Select whether to enable the threshold.
     - **Calculation Type**. You cannot modify the type of calculation.
     - **Count**. Select the number of times that a particular event must occur before the threshold is met.
   - **Threshold Alarm Info**:
     - **Upper/Lower**. You cannot modify the type of threshold.
     - **Threshold**. Modify the threshold. If this threshold is exceeded, the application triggers an alarm.
     - **Severity**. Select whether the alarm is considered critical, major, minor, or informational.
8. Click the **Submit** button.

   The modified alarm configuration displays in the Alarm Configuration table.

View and Manage Alarm Notification Profiles

An alarm notification profile specifies criteria that enable the application to generate and send a notification email message if an alarm occurs. By default, the application does not include any alarm notification profiles.

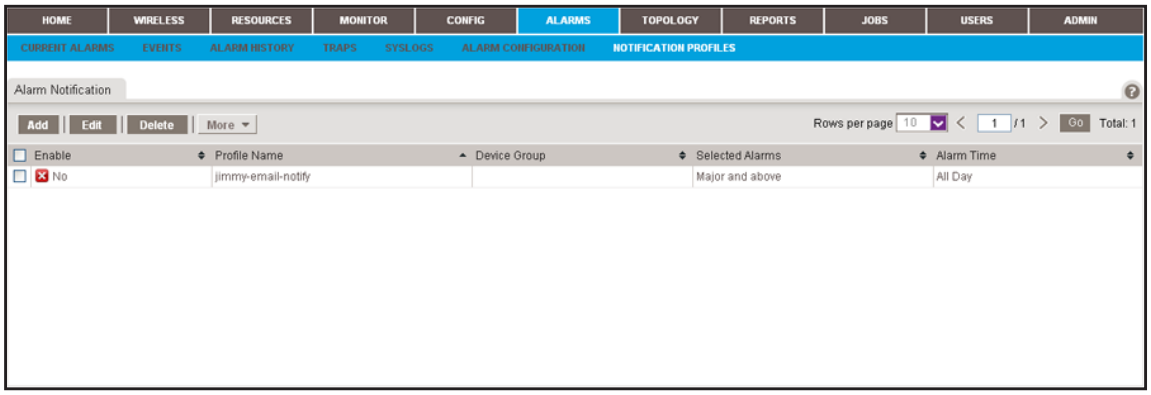
Before the application can generate email messages, you must provide email server settings. For more information, see *Configure the Email Server for Alerts and Alarm Notifications* on page 19.

➢ **To view and manage alarm notification profiles:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > NOTIFICATION PROFILES**.



   If you have not yet added any alarm notification profiles (see *Add or Modify an Alarm Notification Profile* on page 153), the Alarm Notification table is empty.

3. To add columns to or remove them from the Alarm Notification table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Enable, Profile Name, Device Group, Selected Alarms, Alarm Time, Created By, and Create Time.

4. Select an alarm notification profile.
5. Take one of the following actions:
   - Disable the alarm notification profile:
     a. From the **More** menu, select **Disable**.

        A pop-up confirmation screen displays.

     b. Click the **Yes** button.

        The alarm notification profile is disabled and can no longer generate an email message. In the Alarm Notification table, the Enable column displays No for the alarm notification profile.

   - Reenable the alarm notification profile. From the **More** menu, select **Enable**.

     The alarm notification profile is enabled and can generate an email message. In the Alarm Notification table, the Enable column displays Yes for the alarm notification profile.

   - Remove the alarm notification profile:
     a. Select the **Delete** button.

        A pop-up confirmation screen displays.

     b. Click the **Yes** button.

The alarm notification profile is removed from the Alarm Notification table and deleted.

Add or Modify an Alarm Notification Profile

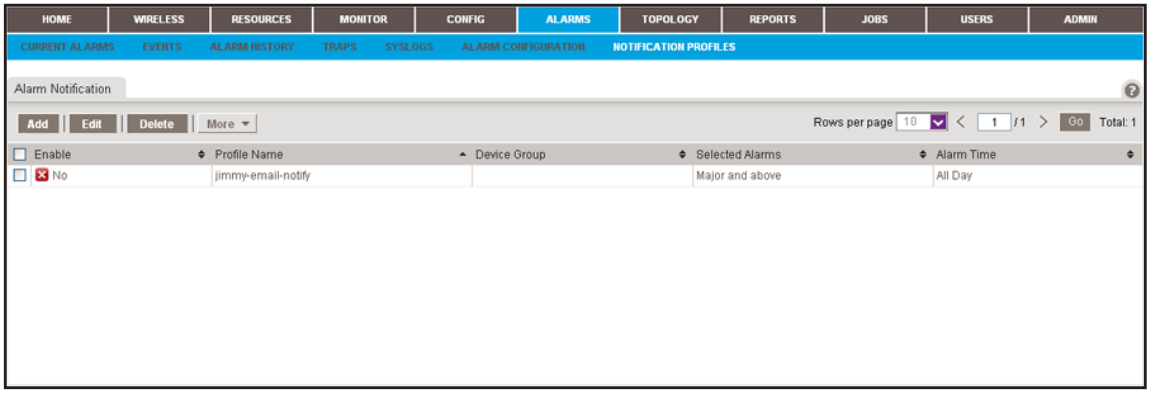
By default, the application does not include any alarm notification profiles. To be notified if an alarm occurs, you must add an alarm notification profile.

➢ **To add an alarm notification profile or modify an existing alarm notification profile:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > NOTIFICATION PROFILES**.

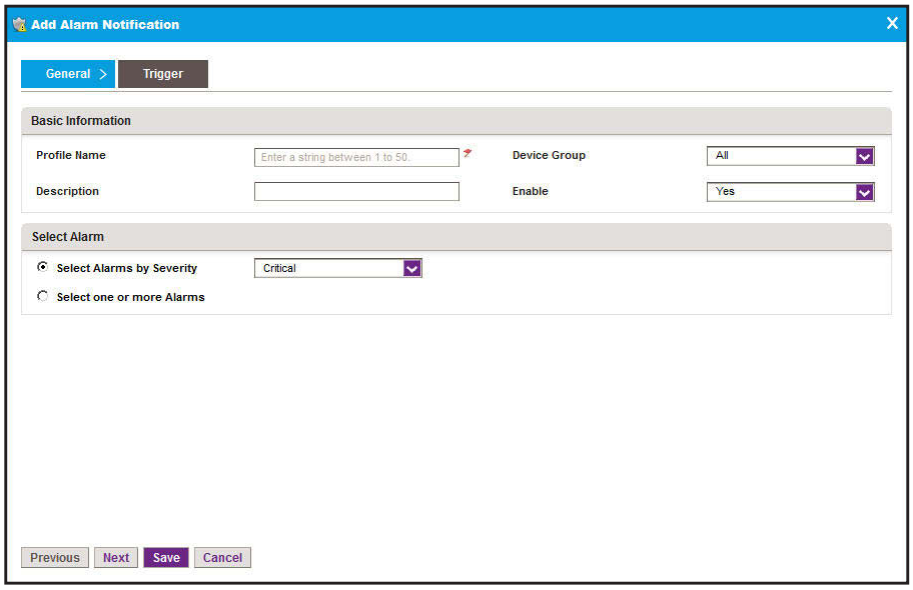


3. To add columns to or remove them from the Alarm Notification table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

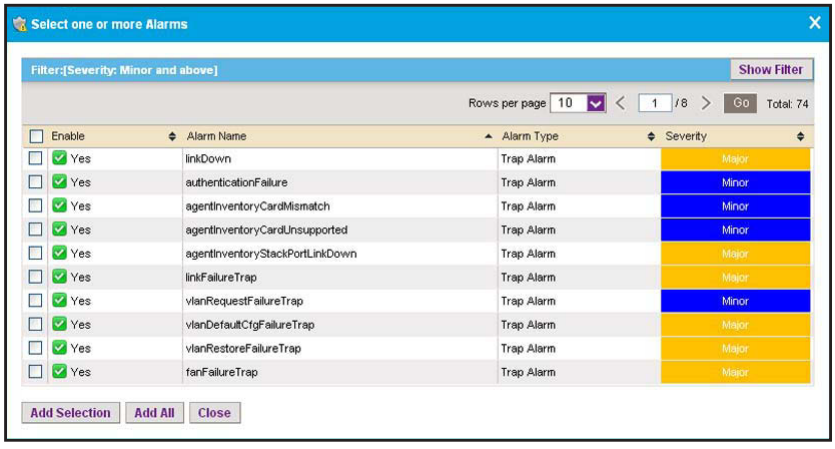
   You can choose from the following columns: Enable, Profile Name, Device Group, Selected Alarms, Alarm Time, Created By, and Create Time.

4. Add an alarm notification profile or modify an existing alarm notification profile:
   - To add an alarm notification profile, click the **Add** button.
   - To modify an existing alarm notification profile:
     a. From the Alarm Notification table, select the alarm notification profile.
     b. Click the **Edit** button.

   For a new alarm notification profile, the Add Alarm Notification screen displays. For an existing alarm notification profile, the Edit Alarm Notification screen displays.



5. In the Basic Information section, specify or modify the following information:
   - **Profile Name**. Enter or modify the name for the profile.
   - **Description**. Enter or modify the description for the profile.
   - **Device Groups**. Select whether to apply the profile to all device groups or to a particular device group.
   - **Enable**. Select whether to enable the alarm notification profile.
6. In the Select Alarm section, select one of the following radio buttons:
   - **Select Alarms by Severity**. Select the alarms by severity by selecting a severity level from the menu.
   - **Select one or more Alarms**. The appearance of the screen changes, enabling you to add alarms:
     a. Click the **Add** button.



     b. Select the alarms that you want to include in the alarm notification profile.

c. Click the **Add Selection** button.

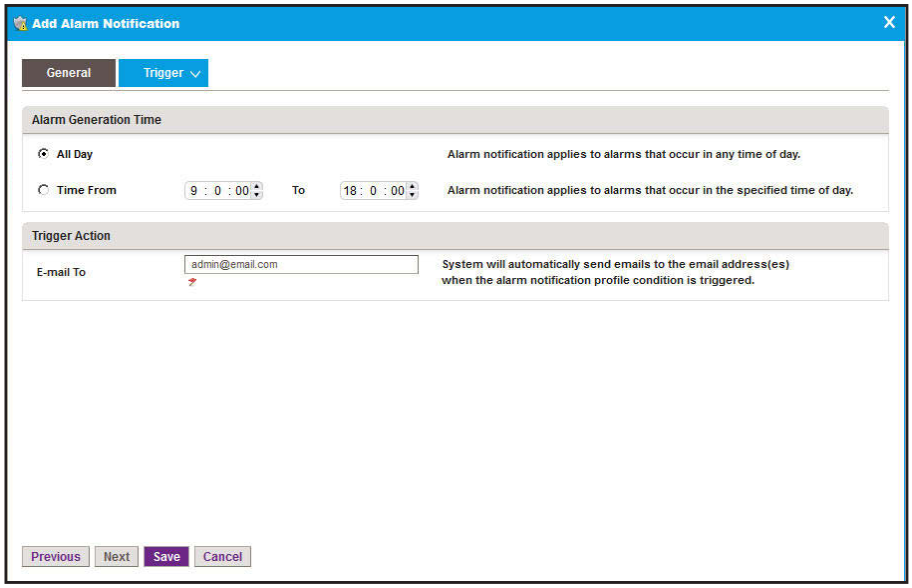
To add all alarms, click the **Add All** button.

The alarms are added to the Add Alarm Notification screen (or, if you are modifying an existing alarm notification profile, to the Edit Alarm Notification screen).

d. If you are modifying an existing alarm notification profile, to remove alarms, select the alarms, and click the **Remove** button.

The alarms are removed from the Edit Alarm Notification screen.

7. Click the **Trigger** tab.



8. Specify or modify the following information:
   - **Alarm Generation Time**. Select one of the following radio buttons:
     - **All Day**. The alarm notification applies to alarms that occur at any time of the day.
     - **Time Frame**. From the menus, select a time frame. The alarm notification applies only to alarms that occur in the specified time frame.
   - **Trigger Action**. Enter the email address to send the notification to if the alarm notification condition is triggered.
9. Click the **Save** button.

The Add Alarm Notification or Edit Alarm Notification screen closes. The alarm profile notification displays in the Alarm Notification table.

Customize Alarm Colors

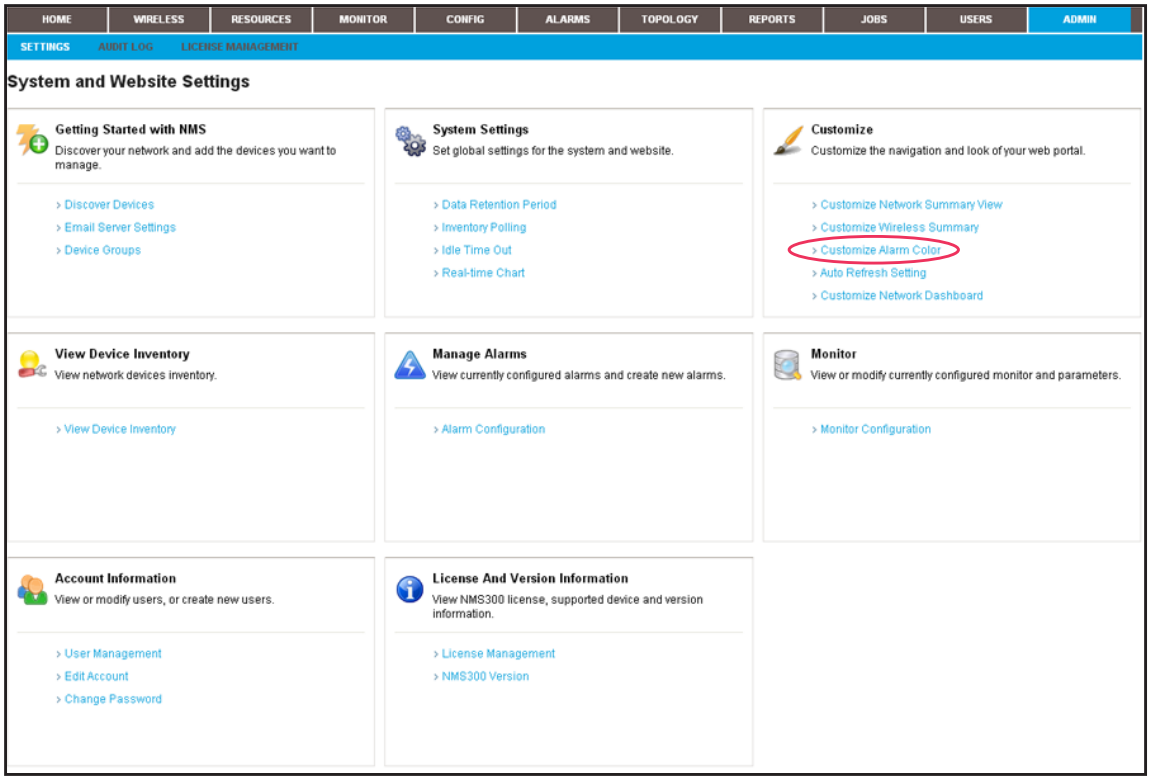
You can change the colors of the alarms.

➢ **To customize the color of an alarm:**

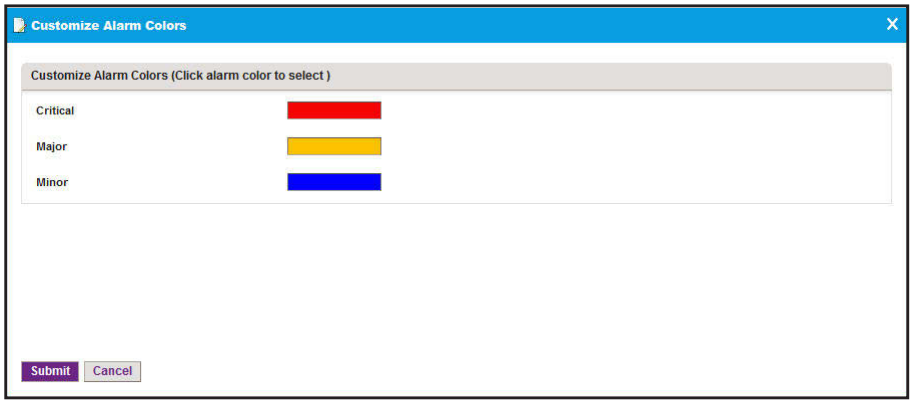
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under Customize, click the **Customize Alarm Color** link.



4. Click the alarm color.

5. Select another color.

6. Click the **Submit** button.

   Your changes are saved.

View and Manage Network Event Notifications

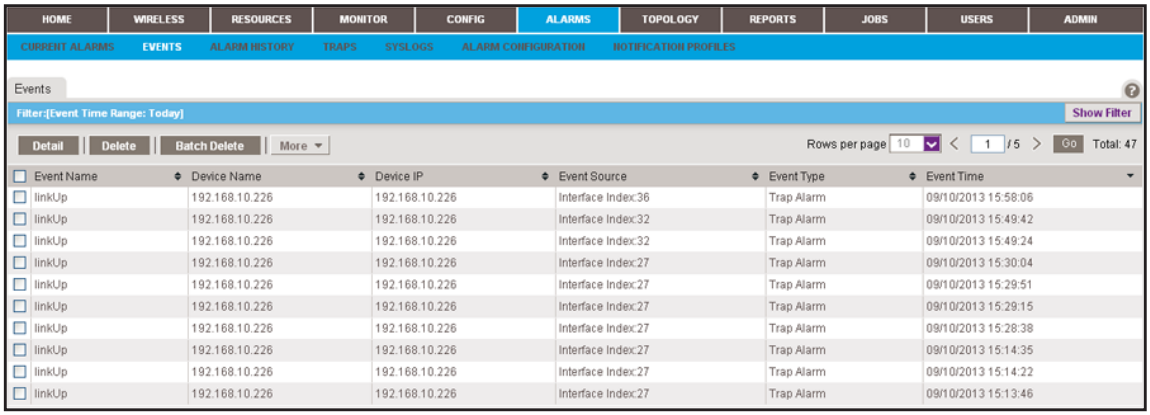
The Events table shows the events for the entire network, including events for devices and interfaces. You can display details about network events, remove network events, and export network events.

➢ **To view and manage network events:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > EVENTS**.



3. To add columns to or remove them from the Events table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

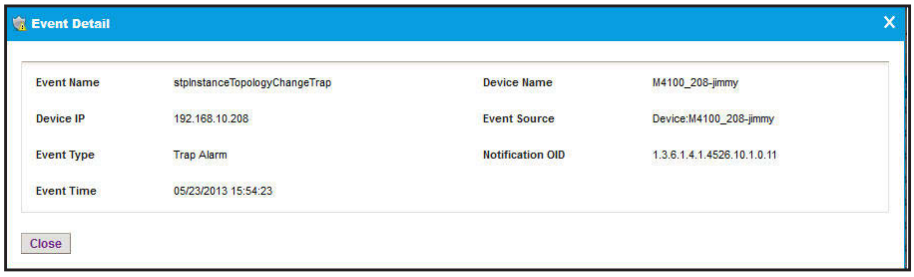
   You can choose from the following columns: Event Name, Device Name, Device IP, Event Source, Event Type, Event Time, and Notification OID.

4. To filter the event entries that are listed, click the **Show Filter** button.

   You can filter the event entries by criteria such as time range, device IP address, and severity level. By default, the event entries are filtered to display today's entries.

   To hide the filter, click the **Hide Filter** button.

5. Take one of the following actions:
   - View details for an event:
     a. Select the event.
     b. Click the **Detail** button.



     c. To close the Event Detail screen, click the **Close** button.
   - Delete an event:
     a. Select the event.
     b. Click the **Delete** button.

        The event is removed from the database.
   - Delete a batch of events:
     a. Select multiple events.
     b. Click the **Batch Delete** button.

        The events are removed from the database.
   - Export the entire Events table to an Excel spreadsheet:
     a. From the **More** menu, select **Export to Excel**.
     b. To save the events on your computer, follow the directions of your browser.
   - Export the entire Events table to a PDF:
     a. From the **More** menu, select **Export to PDF**.
     b. To save the events on your computer, follow the directions of your browser.

View and Manage Device Traps

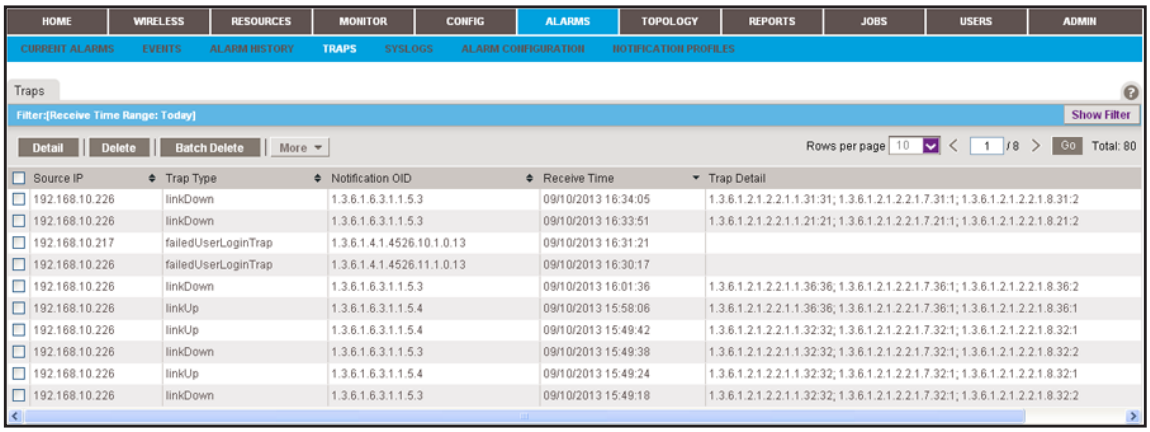
The Traps table shows the device trap events. You can display details about device trap events, remove device trap events, and export device trap events.

➢ **To view and manage device traps:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > TRAPS**.



3. To add columns to or remove them from the Traps table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Source IP, Trap Type, Notification OID, Receive Time, Trap Detail, Trap Version, and Time Stamp.

4. To filter the trap entries that are listed, click the **Show Filter** button.

   You can filter the trap entries by criteria such as time range, device IP address, and severity level. By default, the trap entries are filtered to display today's entries.

   To hide the filter, click the **Hide Filter** button.

5. Take one of the following actions:
   - View details for a trap:
     a. Select the trap.
     b. Click the **Detail** button.

     c. To close the Trap Detail screen, click the **Close** button.
   - Delete a trap:
     a. Select the trap.
     b. Click the **Delete** button.

        The trap is removed from the database.

- Delete a batch of traps:
  a. Select multiple traps.
  b. Click the **Batch Delete** button.

     The traps are removed from the database.
- Export the entire Traps table to an Excel spreadsheet:
  a. From the **More** menu, select **Export to Excel**.
  b. To save the traps on your computer, follow the directions of your browser.
- Export the entire Traps table to a PDF:
  a. From the **More** menu, select **Export to PDF**.
  b. To save the traps on your computer, follow the directions of your browser.

View and Manage Device System Logs

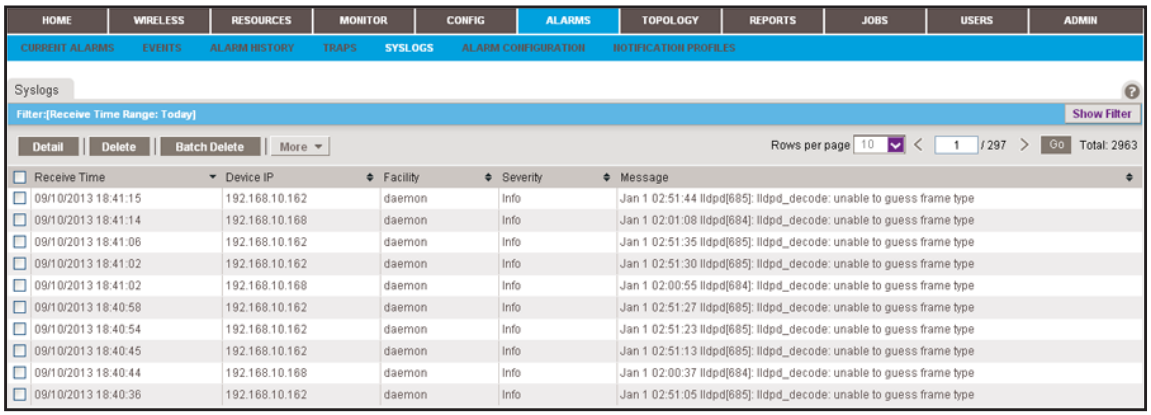
The Syslog table shows the device system log entries. You can display details about log entries, remove log entries, and export log entries.

➢ **To view and manage the device system log entries:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ALARMS > SYSLOGS**.

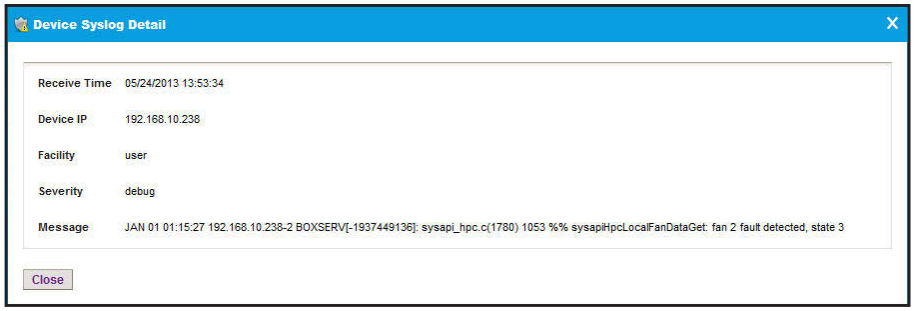

HOME
WIRELESS
RESOURCES
MONITOR
CONFIG
ALARMS
TOPOLOGY
REPORTS
JOBS
USERS
ADMIN
CURRENT ALARMS
EVENTS
ALARM HISTORY
TRAPS
SYSLOGS
ALARM CONFIGURATION
NOTIFICATION PROFILES
Syslogs
Filter:[Receive Time Range: Today]
Show Filter
Detail
Delete
Batch Delete
More
Rows per page 10
1 / 297
Go
Total: 2963
Receive Time
Device IP
Facility
Severity
Message
09/10/2013 18:41:15 192.168.10.162 daemon Info Jan 1 02:51:44 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:41:14 192.168.10.168 daemon Info Jan 1 02:01:08 lldpd[684]: lldpd_decode: unable to guess frame type
09/10/2013 18:41:06 192.168.10.162 daemon Info Jan 1 02:51:35 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:41:02 192.168.10.162 daemon Info Jan 1 02:51:30 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:41:02 192.168.10.168 daemon Info Jan 1 02:00:55 lldpd[684]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:58 192.168.10.162 daemon Info Jan 1 02:51:27 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:54 192.168.10.162 daemon Info Jan 1 02:51:23 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:45 192.168.10.162 daemon Info Jan 1 02:51:13 lldpd[685]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:44 192.168.10.168 daemon Info Jan 1 02:00:37 lldpd[684]: lldpd_decode: unable to guess frame type
09/10/2013 18:40:36 192.168.10.162 daemon Info Jan 1 02:51:05 lldpd[685]: lldpd_decode: unable to guess frame type

3. To filter the syslog entries that are listed, click the **Show Filter** button.

   You can filter the syslog entries by criteria such as time range, device IP address, and severity level. By default, the syslog entries are filtered to display today's entries.

   To hide the filter, click the **Hide Filter** button.

4. Take one of the following actions:
   - View details for a log entry:
     a. Select the log entry.
     b. Click the **Detail** button.


Device Syslog Detail
Receive Time 05/24/2013 13:53:34
Device IP 192.168.10.238
Facility user
Severity debug
Message JAN 01 01:15:27 192.168.10.238-2 BOXSERV[-1937449136]: sysapi_hpc.c(1780) 1053 %% sysapiHpcLocalFanDataGet: fan 2 fault detected, state 3
Close

     c. To close the Device Syslog Detail screen, click the **Close** button.
   - Delete a log entry:
     a. Select the log entry.
     b. Click the **Delete** button.

        The log is removed from the database.
   - Delete a batch of log entries:
     a. Select multiple log entries.
     b. Click the **Batch Delete** button.

        The log entries are removed from the database.
   - Export the entire Syslogs table to an Excel spreadsheet:
     a. From the **More** menu, select **Export to Excel**.
     b. To save the log entries on your computer, follow the directions of your browser.
   - Export the entire Syslogs table to a PDF:
     a. From the **More** menu, select **Export to PDF**.
     b. To save the log entries on your computer, follow the directions of your browser.

7. Manage Maps and Topologies

View the topology of your network

You can create hierarchical maps and topological views of your network.

This chapter covers the following topics:

- *View and Manage Maps*
- *View and Manage Network Topologies*

View and Manage Maps

The application provides a default world map. This map is the root map for any child map that you add.

The following sections describe the tasks that relate to maps:

- *View a Hierarchical Map and Locate a Device*
- *Manage a Hierarchical Map*
- *Add a Childmap*
- *Add Devices to a Map*
- *Add a Link Between Devices on a Map*
- *Customize the Style of a Link on a Map*

View a Hierarchical Map and Locate a Device

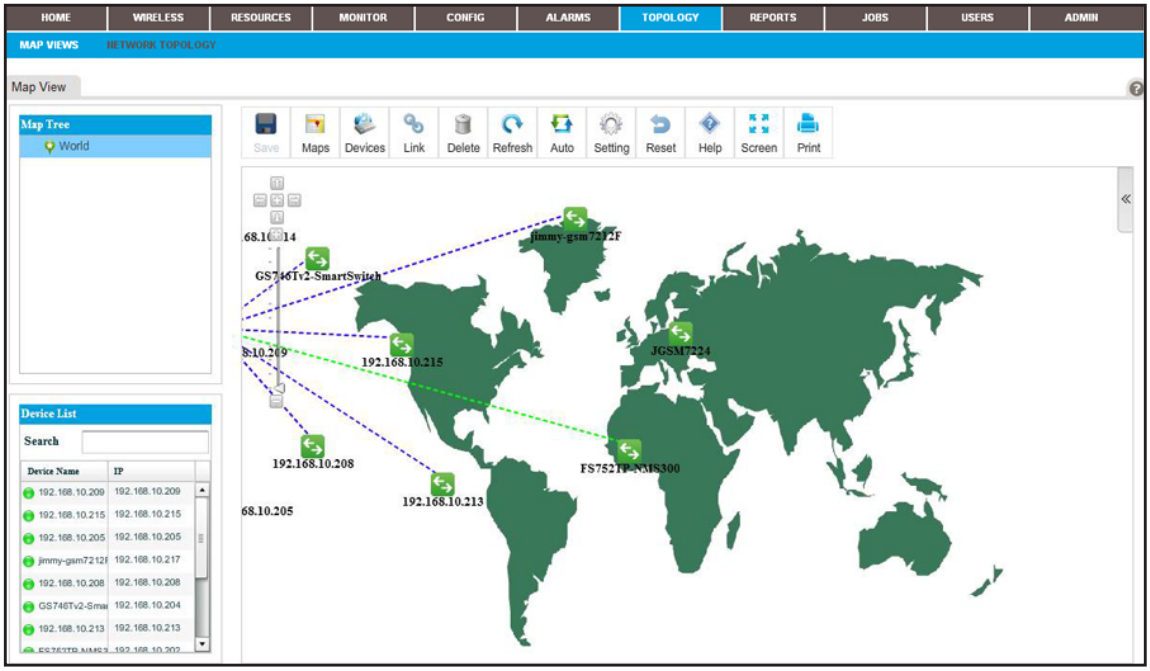
You can view a hierarchical map of your network, locate devices on the map, and view details about the devices, including alarms.

➢ **To view a hierarchical map, locate a device on the map, and view details about the device:**

1. Log in to the application.

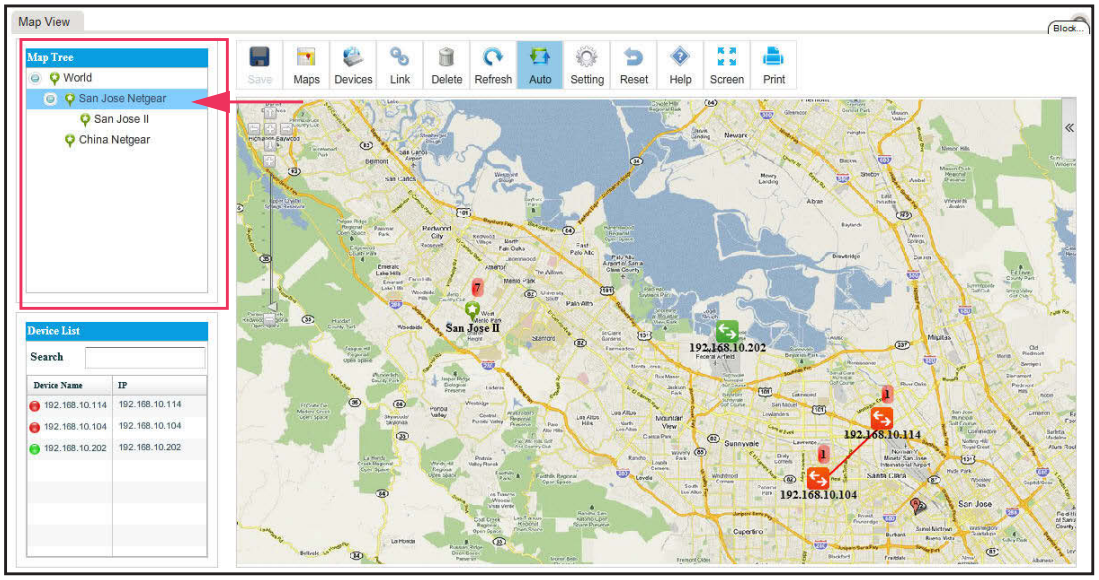
   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > MAP VIEWS**.



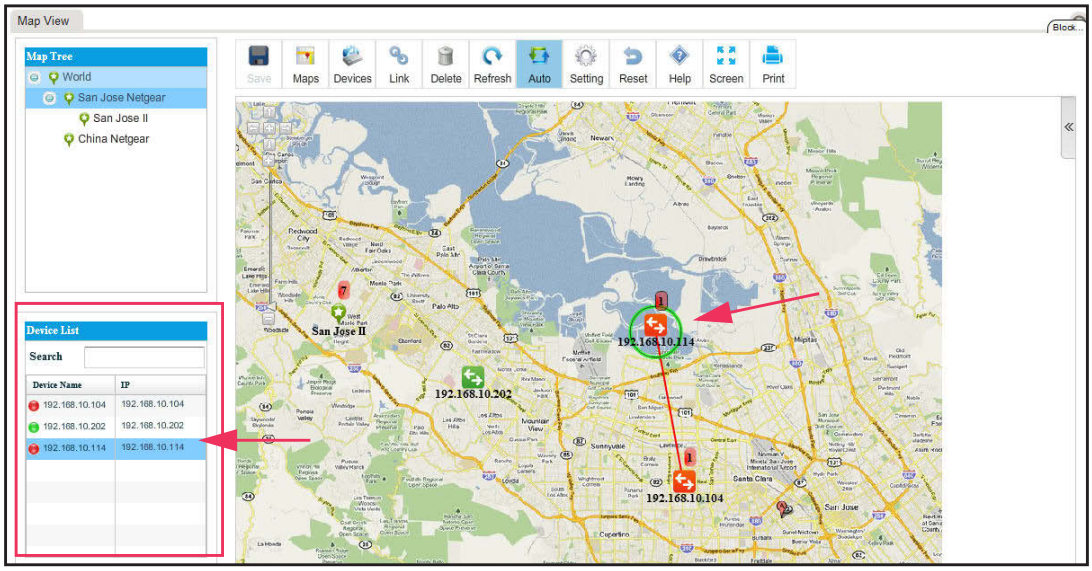
3. From the Map Tree, select the map.

The selected map displays.



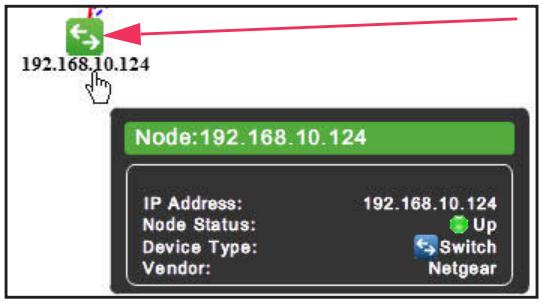
4. From the Device List table, select the device that you want to locate on the map.

   A circle displays around the selected device.



5. To view information about the device (node), point to the device on the map.

A pop-up screen similar to the following displays.

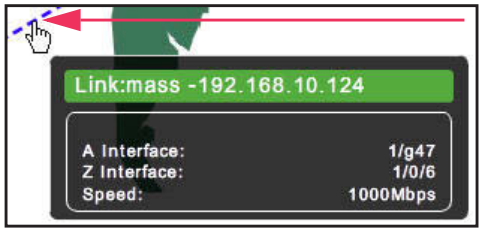


6. To see detailed information and the Dashboard menu for the device, double-click the device on the map.

   For more information, see *View Device Details and Interface Details* on page 77.

7. To view the details for a link, point to the link on the map.

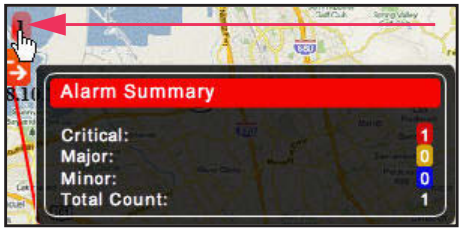
   A pop-up screen similar to the following displays.



8. To view the summary for an alarm, point to the alarm summary on the map.

   An alarm summary is displayed as a red-colored rectangular with a number.

   A pop-up screen similar to the following displays.



Manage a Hierarchical Map

On the Map Views screen, the icons that display above a map let you perform various tasks.

Figure 3. Icons on the Map Views screen

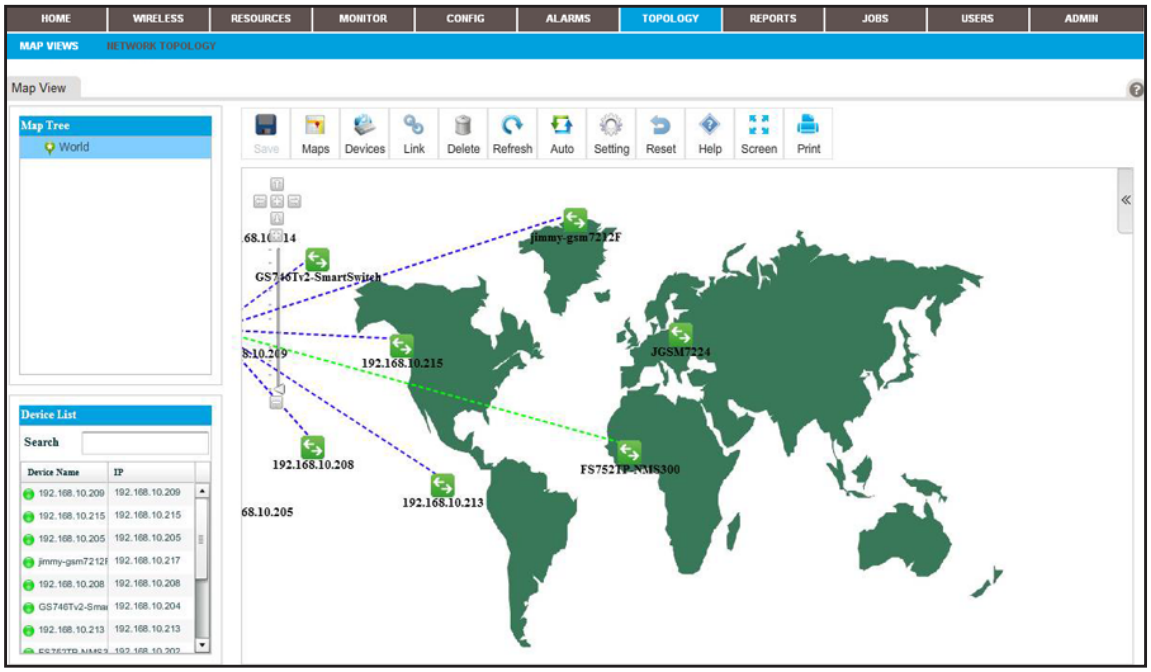
The following procedure describes the tasks that you can perform for a hierarchical map. For complicated tasks, the procedure points to a section that provides detailed information.

➢ **To manage a hierarchical map:**

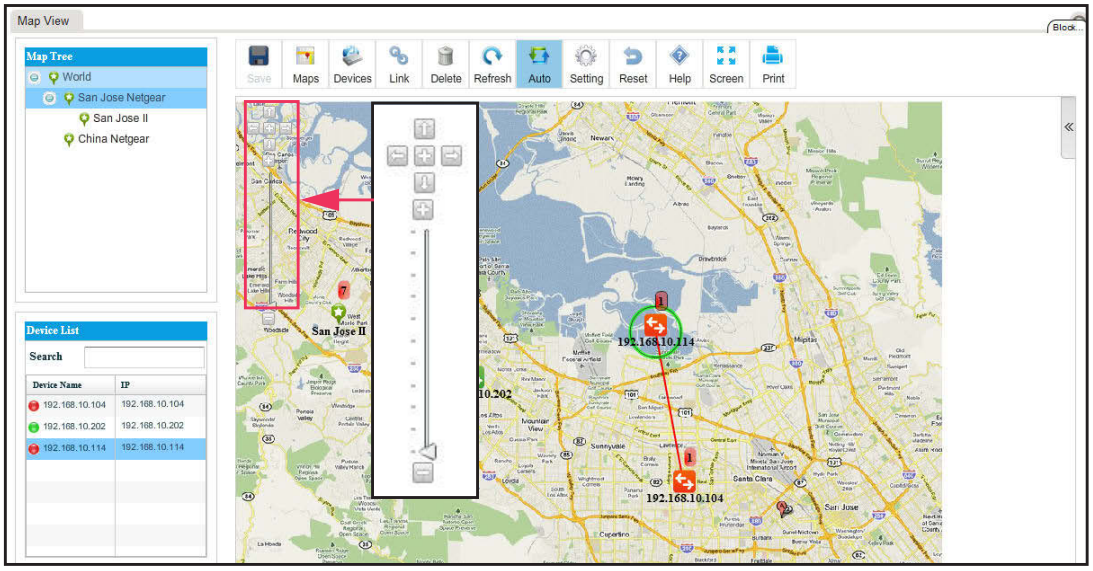
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > MAP VIEWS**.



3. From the Map Tree, select the map.
4. To rescale the map, use the scaling tool that displays on the left of the map.



5. To reposition the map, hold your cursor on the map and drag the map to a new position.

6. Take one of the following actions:
   - Let the application refresh the map automatically. Click the **Auto** icon.

     The map refreshes automatically every two minutes. Automatic refreshment is the default setting.
   - Refresh the map manually. Click the **Refresh** icon.

     The map refreshes once immediately.
   - Add a childmap. Click the **Maps** icon.

     For more information, see *Add a Childmap* on page 168.
   - Add devices to a map. Click the **Devices** icon.

     For more information, see *Add Devices to a Map* on page 169.
   - Add a link between devices on a map. Click the **Link** icon.

     For more information, see *Add a Link Between Devices on a Map* on page 171.
   - Customize the link style settings. Click the **Setting** icon.

     For more information, see *Customize the Style of a Link on a Map* on page 174.
   - Remove a childmap, device, or link from the map:
     a. Select the item.
     b. Click the **Delete** icon.

        The item is removed.
   - Undo unsaved changes. Click the **Reset** icon.

     The unsaved changes are reset.
   - Save changes. Click the **Save** icon.

     Your changes are saved. When the Save icon is grayed out, everything is saved.
   - Open the Help screen. Click the **Help** icon.

     The Help pop-up screen displays.
   - Enter full-screen mode. Click the **Screen** icon.

     The screen displays in full-screen mode. To return to the regular screen display, either press the **Esc** key, or from the full screen, click the **Screen** icon.
   - Print the screen. Click the **Print** icon.

     The map is printed.

Add a Childmap

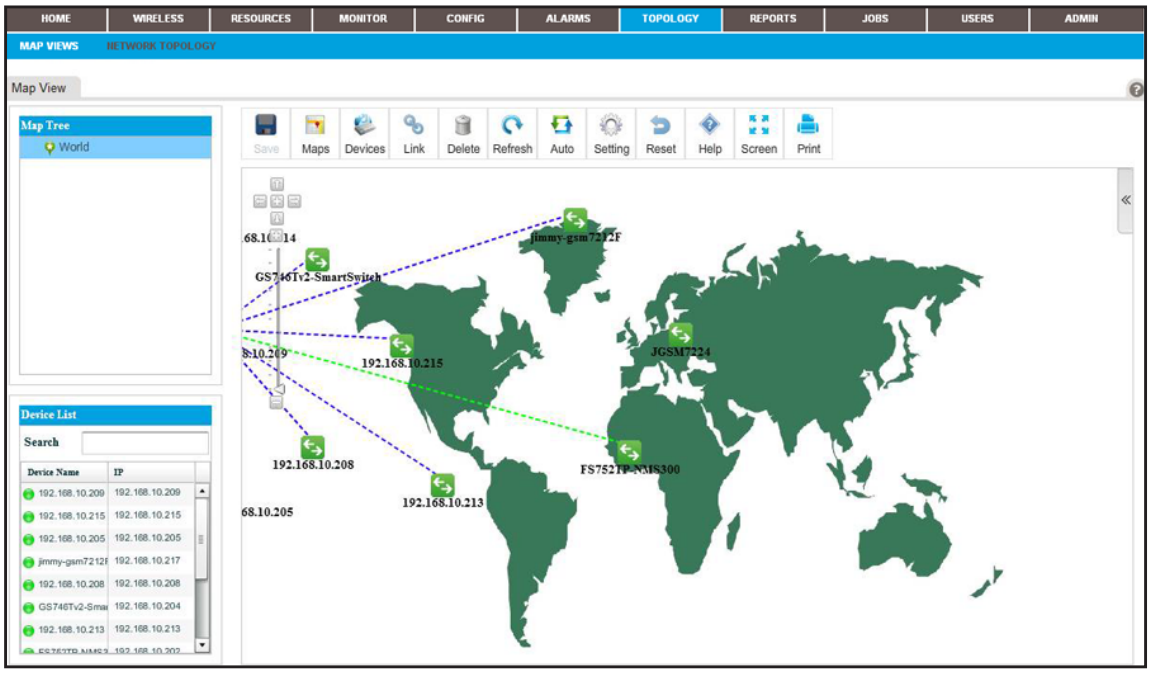
You can add a childmap (submap) to a hierarchical map. The hierarchical map functions as the parent map to the childmap. The application provides default childmaps. You can also import your own childmaps.

➢ **To add a childmap:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

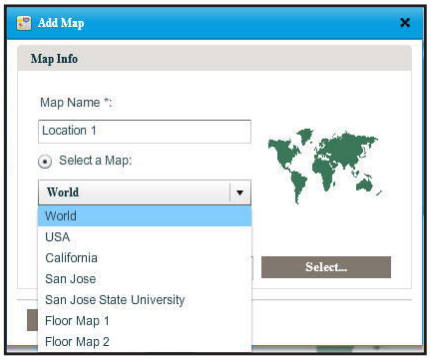
2. Select **TOPOLOGY > MAP VIEWS**.



3. From the Map Tree, select the map.
4. Click the **Maps** icon.

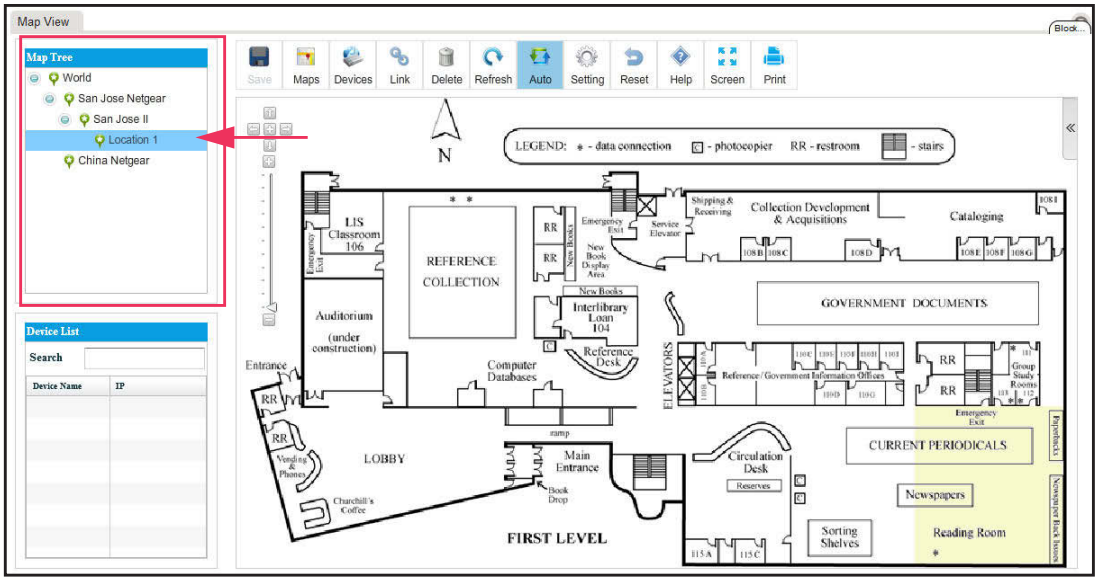
The Add Map screen displays.

5. Enter a name for the childmap.



6. Either select a default childmap or import a map from your computer by selecting one of the following radio buttons:
   - **Select a Map**. Select a default map from the menu.
   - **Select a Local Map**. Take the following action:
     a. Click the **Select** button.
     b. Locate and select a map on your computer.
7. Click the **OK** button.

   The map that you selected or imported displays as a childmap below the parent map and the name of the map you selected displays in the Map Tree.



Add Devices to a Map

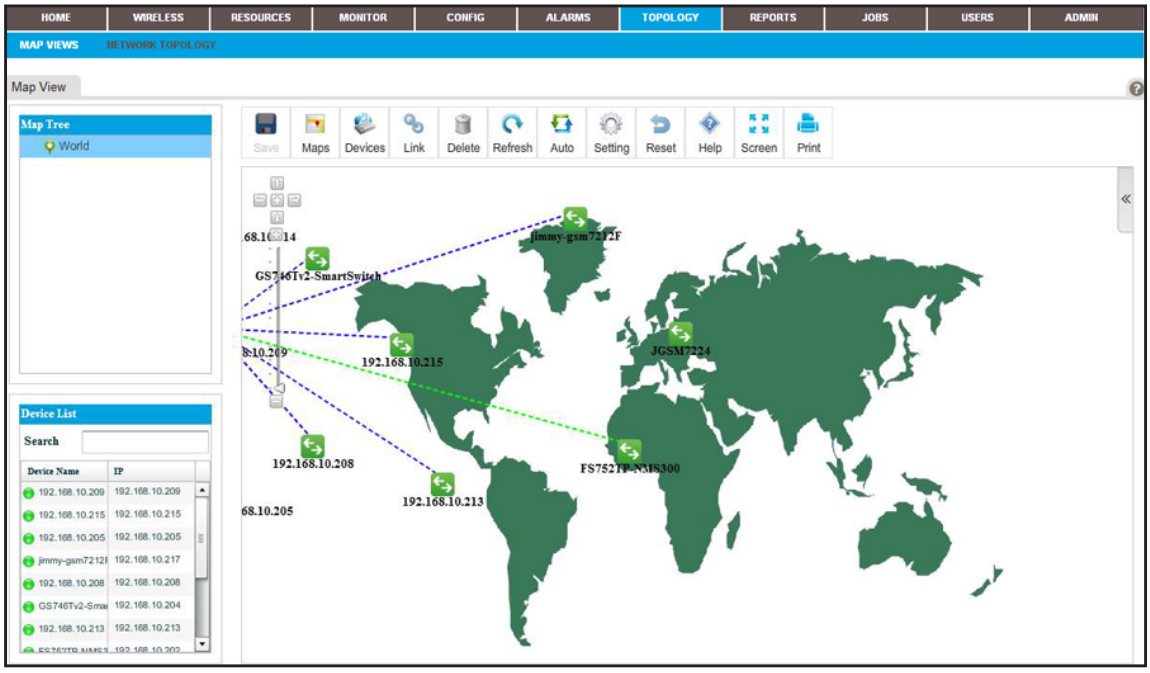
You can add devices to a map.

➢ **To add devices to a map:**

1. Log in to the application.

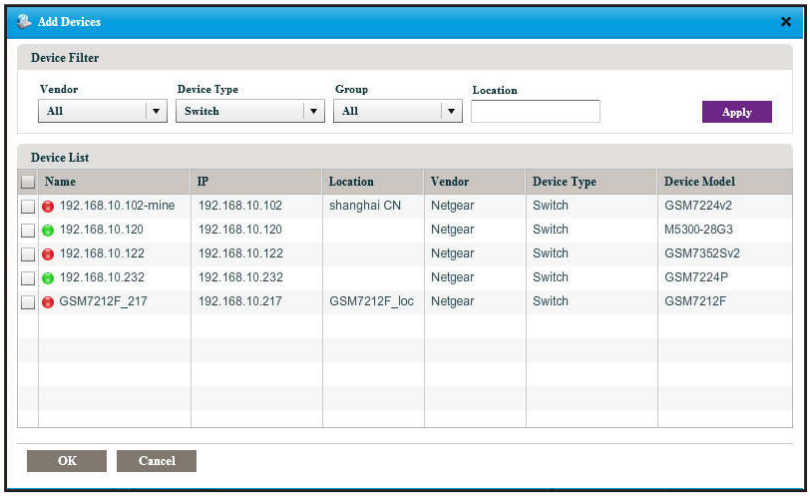
   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > MAP VIEWS**.



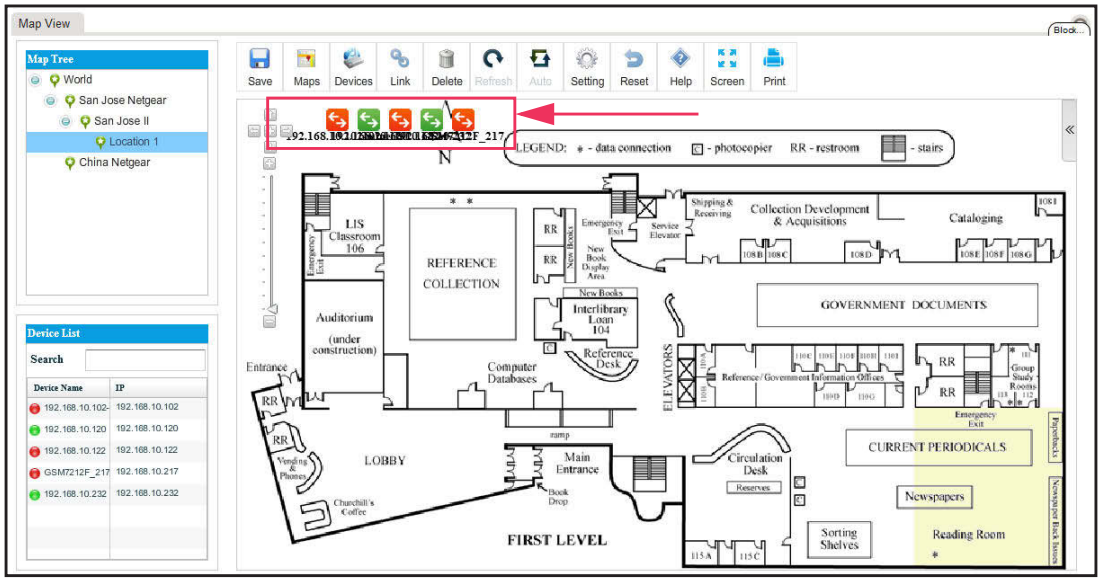
3. From the Map Tree, select the map.
4. Click the **Devices** icon.

The Add Devices screen displays.



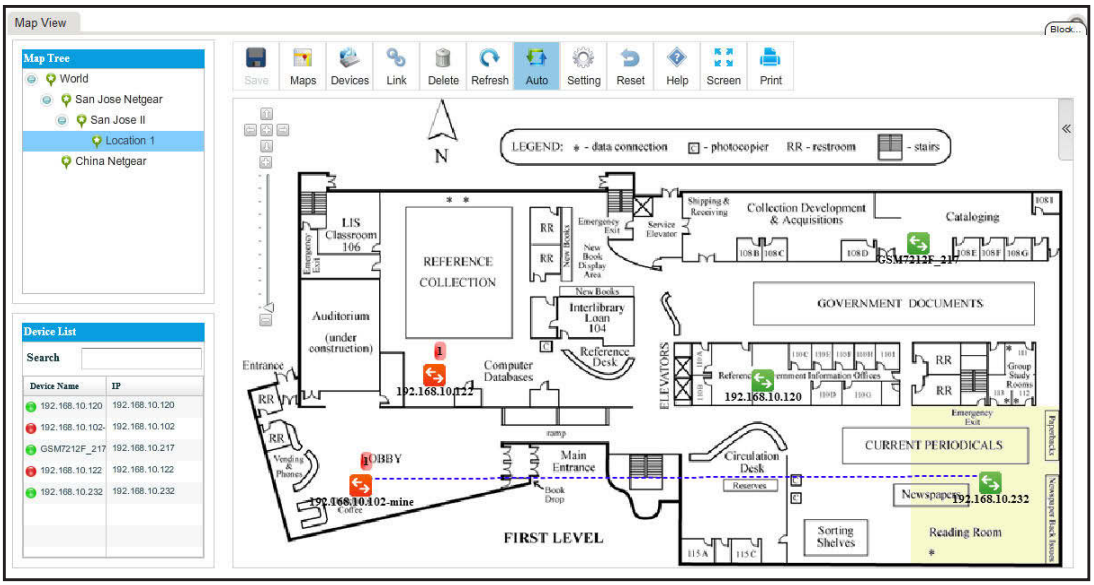
5. Select one or more devices.
6. Click the **OK** button.

The devices display on the map.



7. For each device, select the device and drag it to where you want it on the map.
8. Click the **Save** button.

   The devices display at their locations on the map. The map also displays the existing links between the devices.



Add a Link Between Devices on a Map

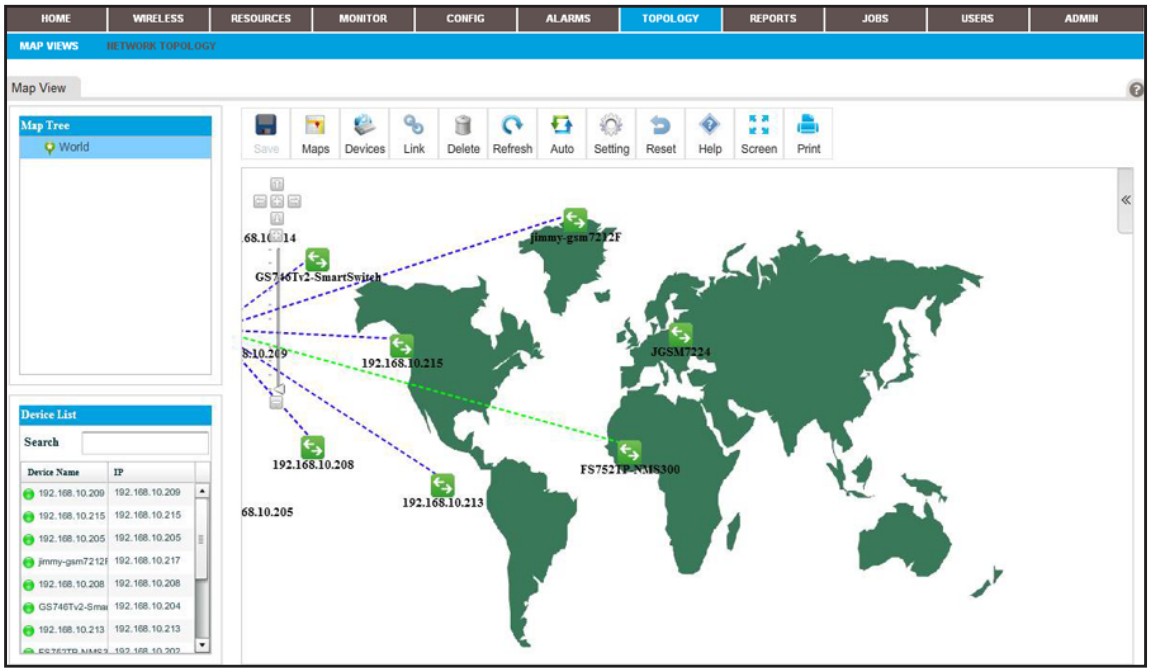
You can add a link between devices. For devices that do not support link discovery through Link Layer Discovery Protocol (LLDP), you can manage links manually. When you know that physical connections exist for the non-LLDP devices, you can draw these links manually and also update them manually when the physical connections are reconfigured.

➢ **To add a link between devices on a map:**

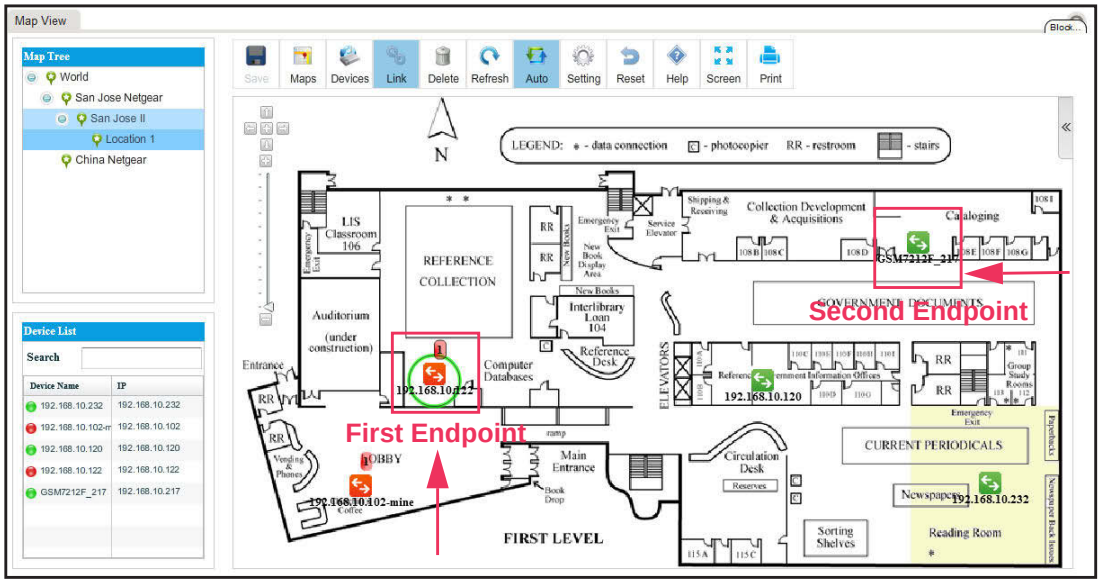
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > MAP VIEWS**.



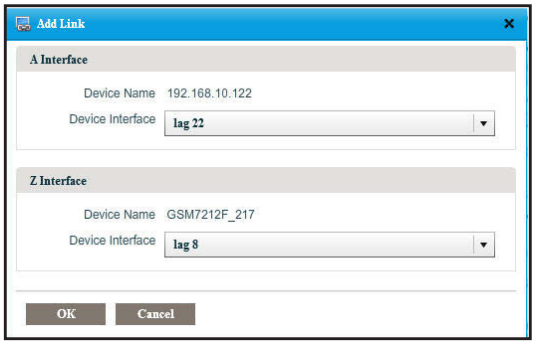
3. From the Map Tree, select the map.
4. Select the device that is the first endpoint of the link.



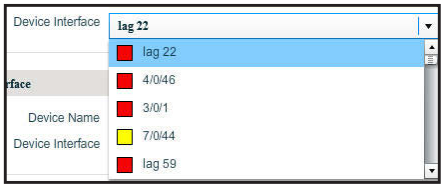
5. Click the **Link** icon.

6. Drag your cursor from the device that you selected in *Step 4* to the device that is the second endpoint of the link.
7. Release the mouse button.

   The Add Link screen displays.



8. From the menus, select the device interface for each end of the link.

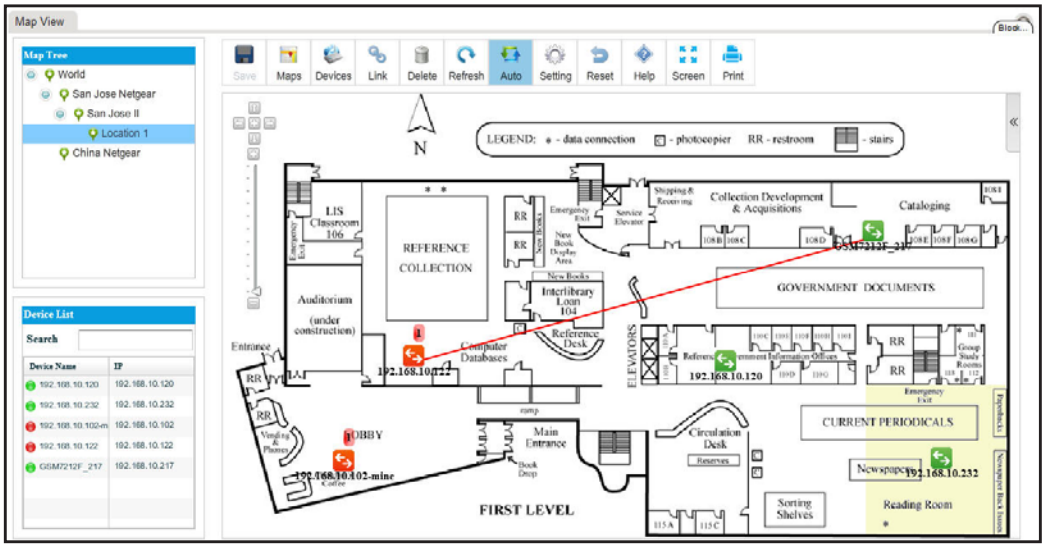


9. Click the **OK** button.

   The Add Link screen closes.

10. Click the **Save** button.

    The link is added.



Customize the Style of a Link on a Map

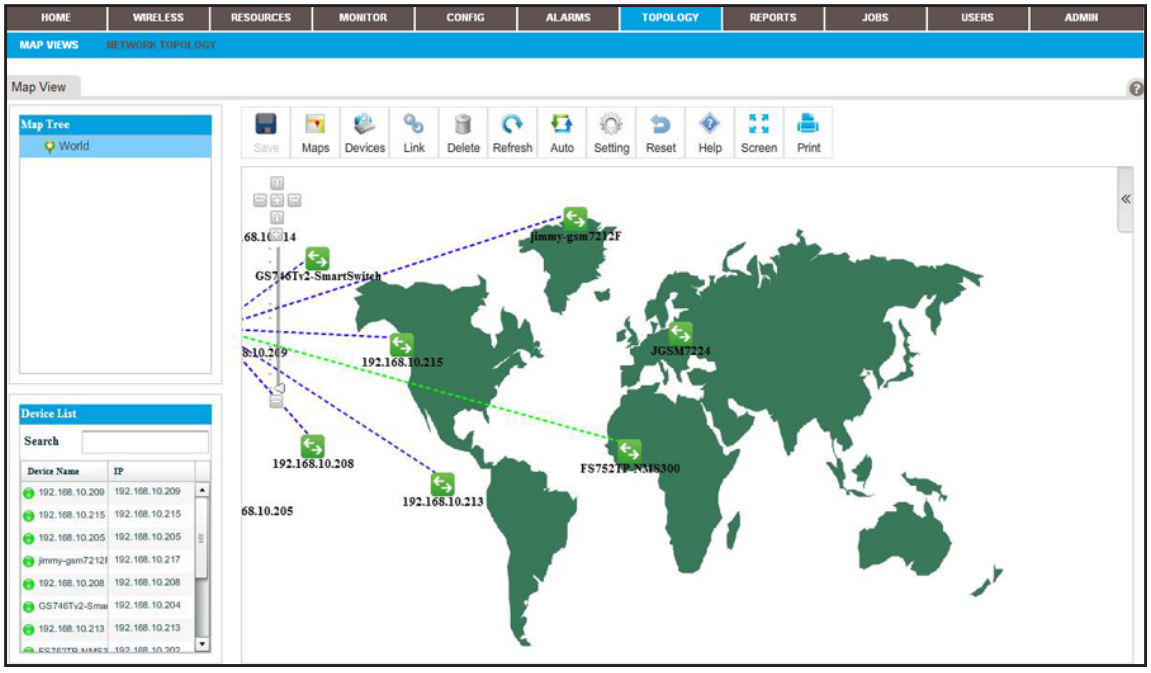
You can customize the way that a link displays.

➢ **To customize the style of a link:**

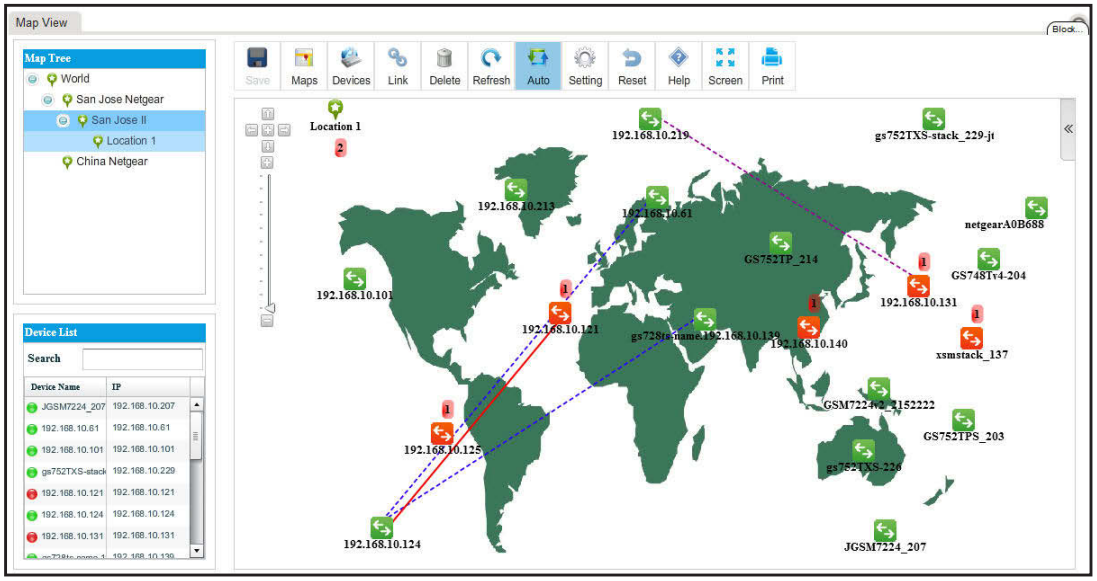
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > MAP VIEWS**.

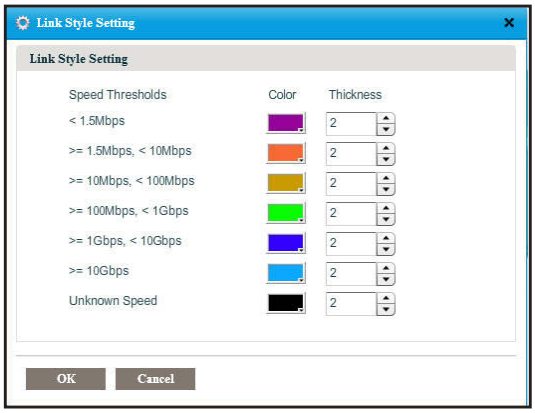


3. From the Map Tree, select the map.

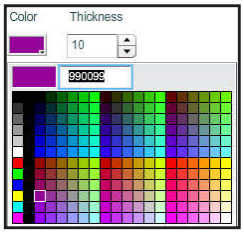


4. Click the **Setting** icon.

The Link Style Setting screen.

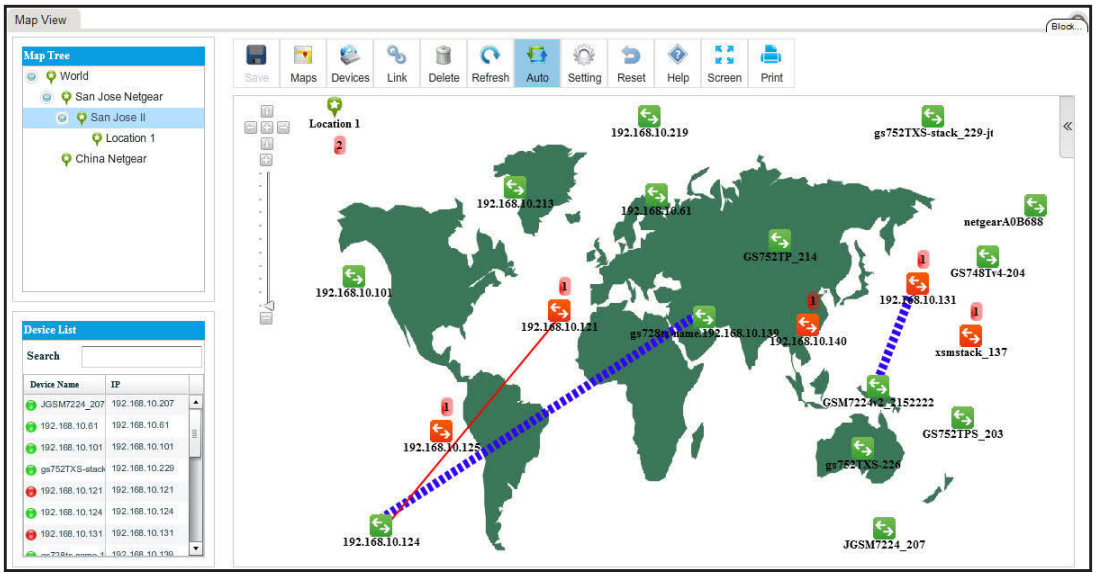


5. Select the color and thickness of the links:



6. Click the **OK** button.

The links on the map display the modified link styles.



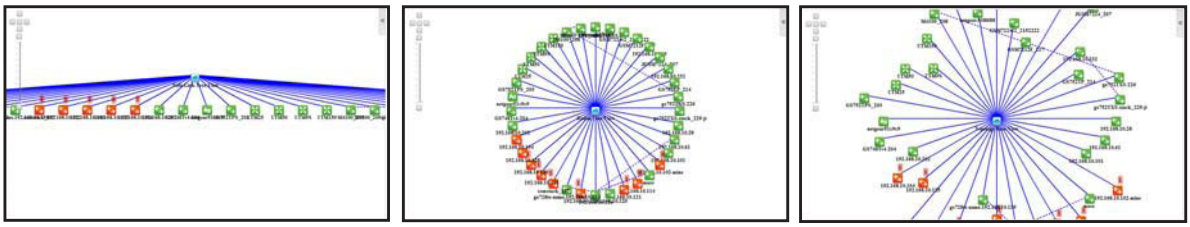
7. Click the **Save** button.

Your changes are saved.

View and Manage Network Topologies

A network topology displays the structure of your network as a link tree view, radial view, or spring view:

- **Link tree view**. The network nodes are displayed as a hierarchical organization chart.
- **Radial view**. The network nodes are displayed in an outwardly expanding radial pattern.
- **Basic spring view**. The network nodes are displayed in a pattern in which children nodes are in circles with parent nodes.



Link tree view | Radial view | Basic spring view

Figure 4. Network topology views

The following sections describe the tasks that relate to network topology views:

- *Add a Topology View*
- *View a Network Topology and Details About a Device*
- *Manage a Topology View*
- *Add a Link Between Devices on a Topology View*
- *Customize the Style of a Node and Link on a Topology View*
- *Remove a Topology View*

Add a Topology View

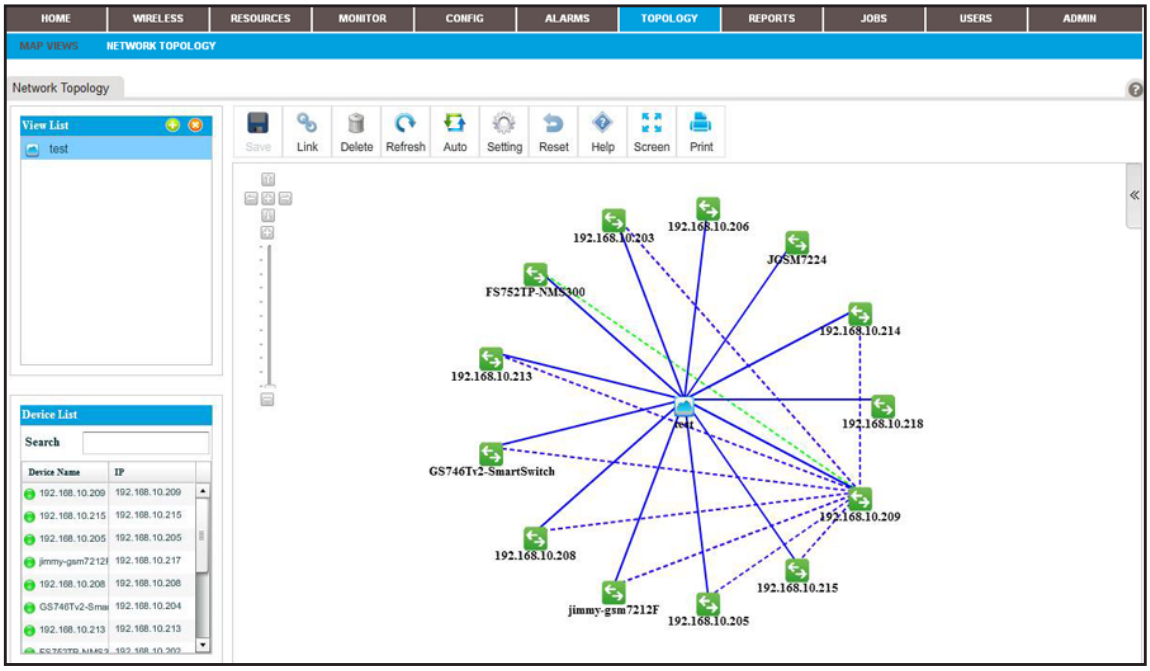
You can add a topology view of your network.

➢ **To add a topology view of your network:**

1. Log in to the application.

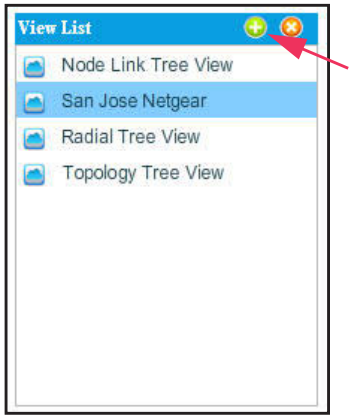
   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > NETWORK TOLOPOGY**.

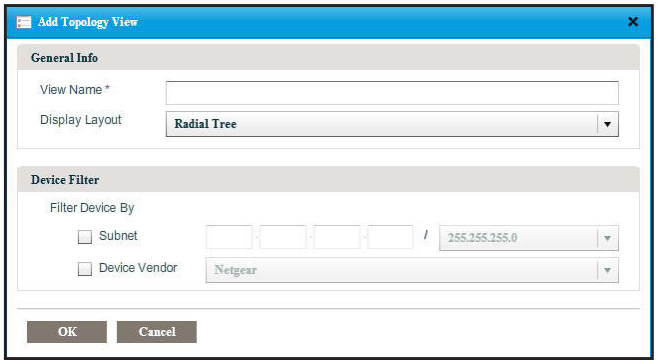


Note: *If you have not yet added any topology views for your network, the screen does not display any.*

3. Next to View List, click the **+** () button.



The Add Topology View screen displays.



4. Specify the following information:
   - **General Info**:
     - **View Name**. Enter a name for the topology view.
     - **Display Layout**. From the menu, select **Radial**, **Node Tree**, or **Basic Spring**.
   - **Device Filter**. Select one of the following check boxes and specify the corresponding information:
     - **Subnet**. Enter an IP address and select a subnet from the menu.
     - **Device Vendor**. Select a vendor from the menu.
5. Click the **OK** button.

   The Add Topology View screen closes.
6. To view the new topology view, select it from the View List table.

   The topology view displays.

View a Network Topology and Details About a Device

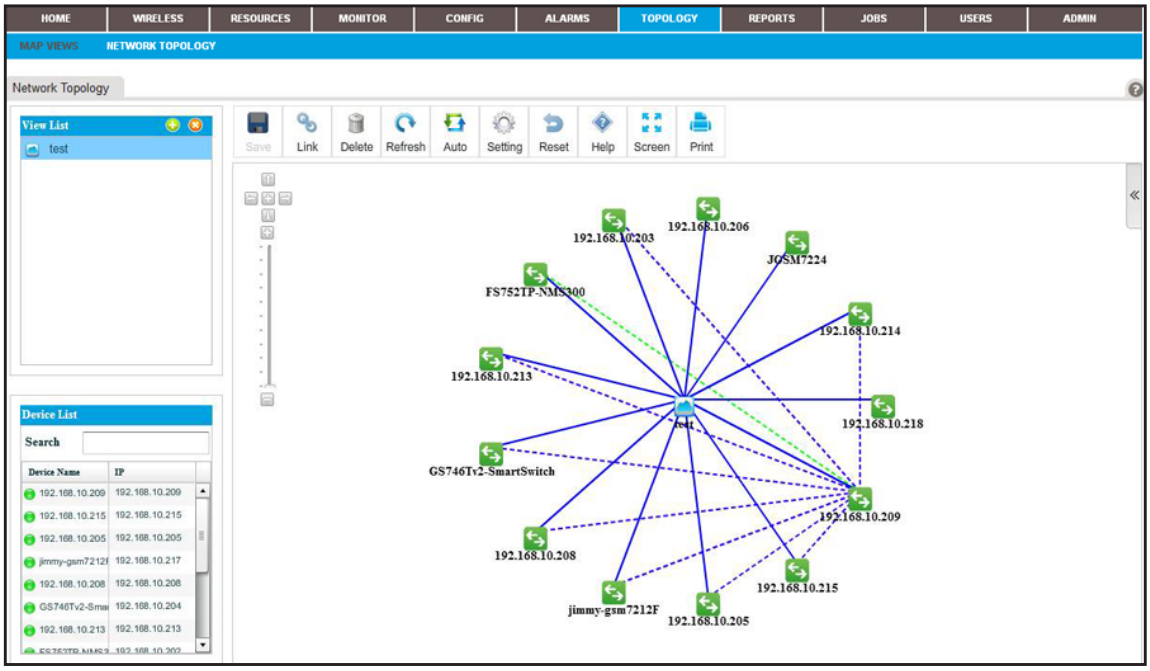
You can view a network topology and view details about the devices, including alarms.

➢ **To display a network topology and details about a device in the network:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

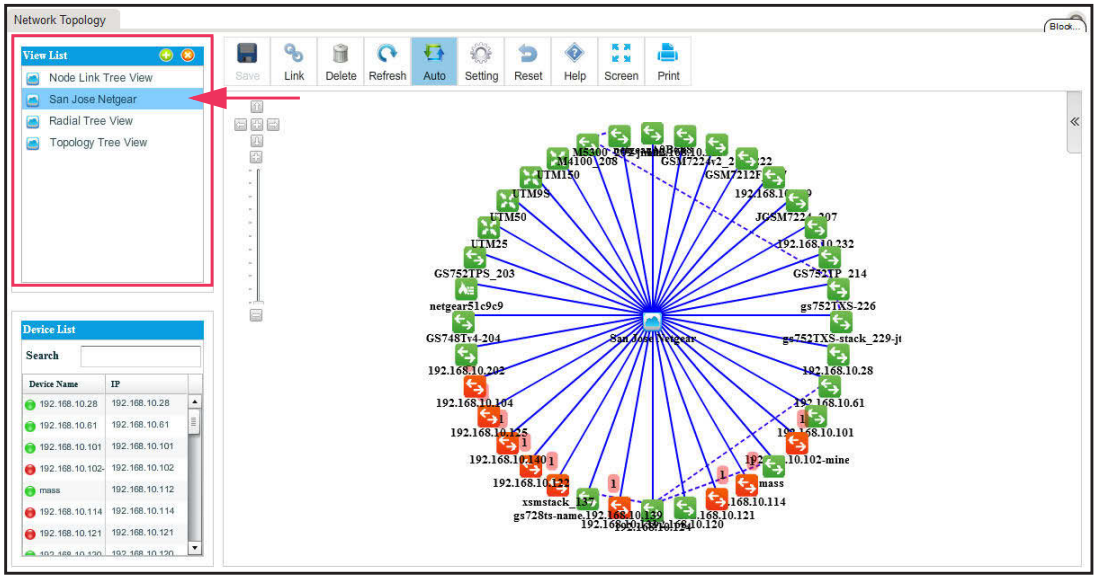
2. Select **TOPOLOGY > NETWORK TOPOLOGY**.



3. From the View List table, select the topology view.

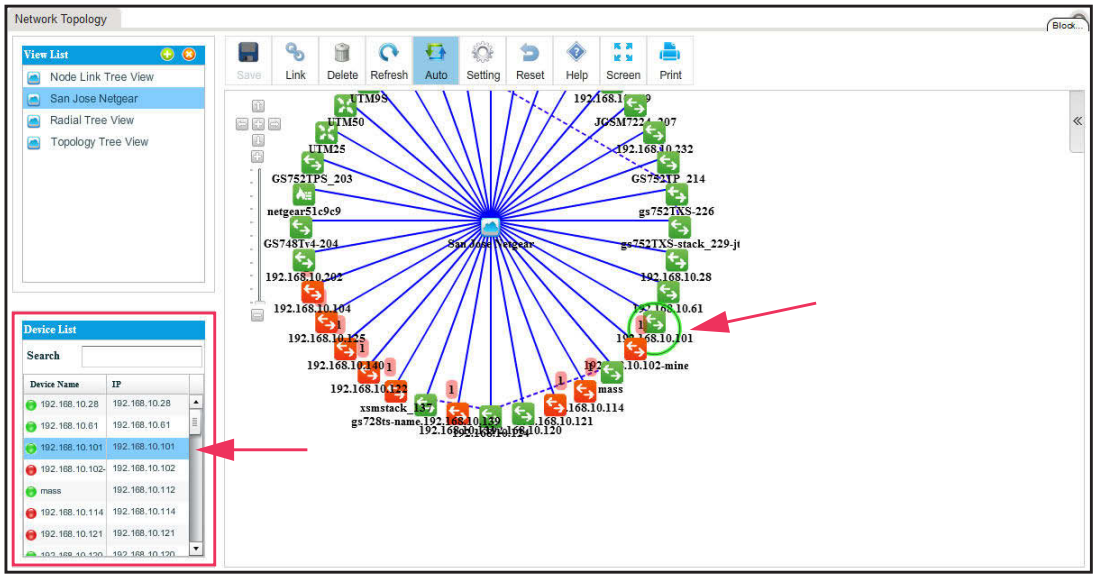
   For information about adding a topology view, see *Add a Topology View* on page 176.

   The selected view displays.



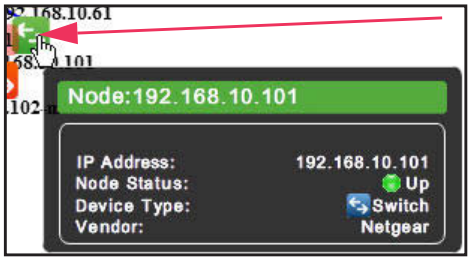
4. From the Device List table, select a device.

A circle displays around the selected device.



5. To view information about the device (node), point to the device on the map.

   A pop-up screen similar to the following displays.

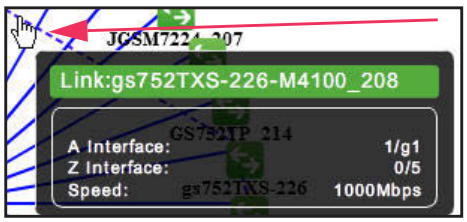


6. To see detailed information and the Dashboard menu for the device, double-click the device on the map.

   For more information, see *View Device Details and Interface Details* on page 77.

7. To view the details for a link, point to the link on the map.

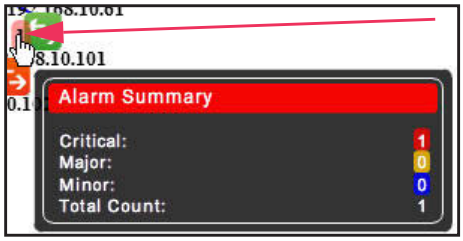
   A pop-up screen similar to the following displays.



8. To view the summary for an alarm, point to the alarm summary on the map.

   An alarm summary is displayed as a red-colored rectangular with a number.

A pop-up screen similar to the following displays.



Manage a Topology View

On the Network Topology screen, the icons that display above a topology view let you perform various tasks.

Figure 5. Icons on the Network Topology screen

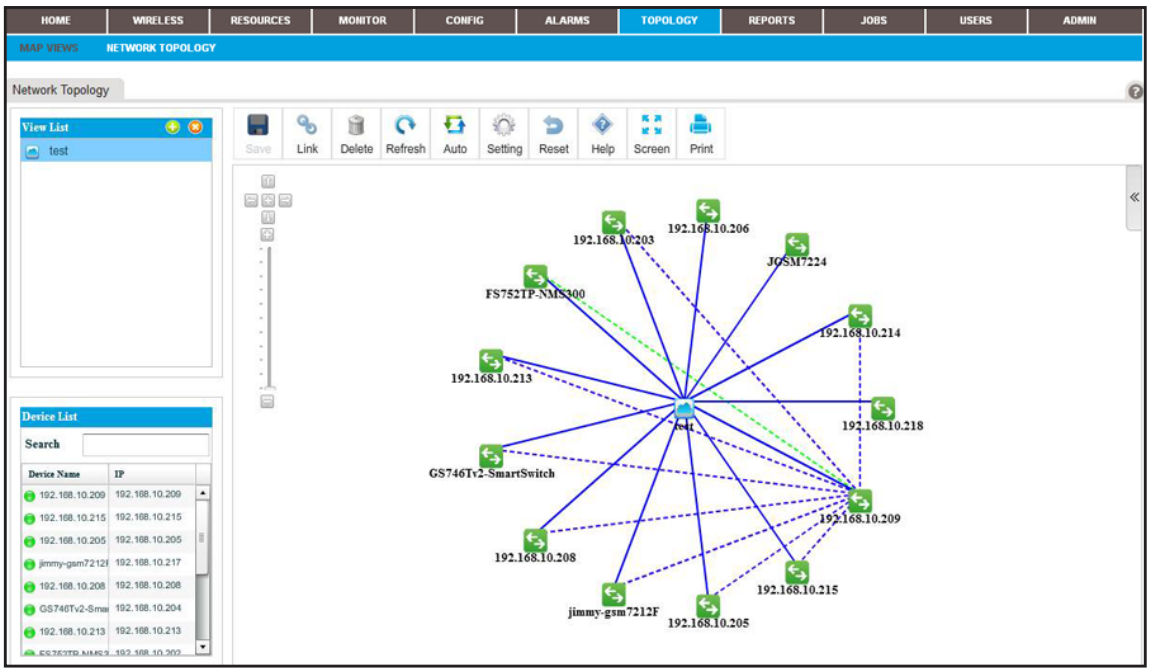
The following procedure describes the tasks that you can perform for a topology view. For complicated tasks, the procedure points to a section that provides detailed information.

➢ **To manage a topology view:**

1. Log in to the application.

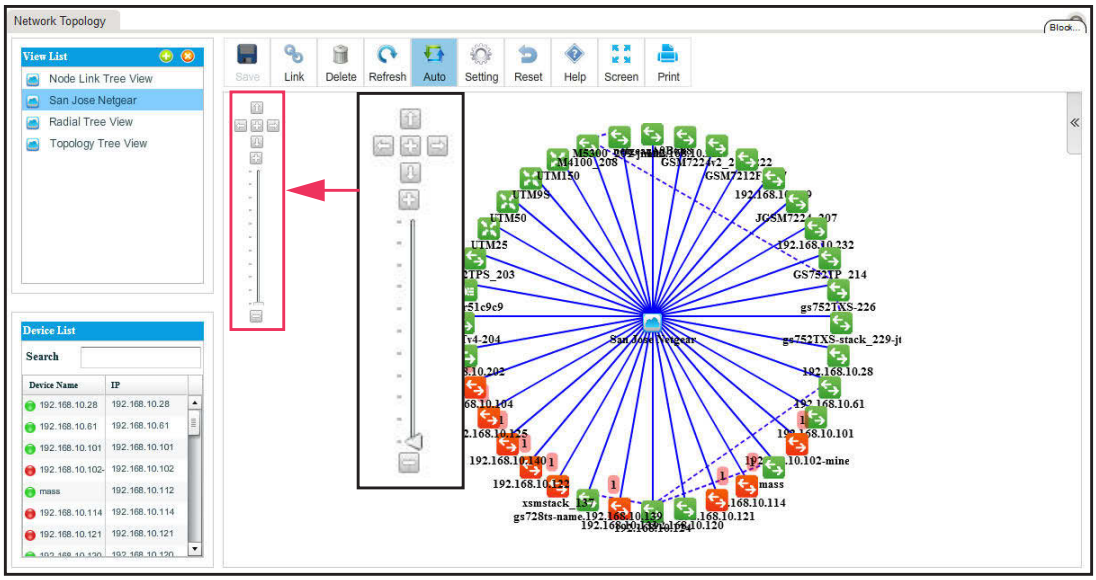
   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > NETWORK TOPOLOGY**.



3. From the View List table, select the topology view.

4. To rescale the topology view, use the scaling tool that displays on the left of the topology view.



5. To reposition the topology view, hold your cursor on the topology view and drag the topology view to a new position.
6. Take one of the following actions:
   - Let the application refresh the topology view automatically. Click the **Auto** icon.

     The topology view refreshes automatically every two minutes. Automatic refreshment is the default setting.
   - Refresh the topology view manually. Click the **Refresh** icon.

     The topology view refreshes once immediately.
   - Add a link between devices on a topology view. Click the **Link** icon.

     For more information, see *Add a Link Between Devices on a Topology View* on page 183.
   - Customize the link style settings. Click the **Setting** icon.

     For more information, see *Customize the Style of a Node and Link on a Topology View* on page 185.
   - Remove a link from the topology view:

     a. Select the link.

     b. Click the **Delete** icon.

     The link is removed.
   - Undo unsaved changes. Click the **Reset** icon.

     The unsaved changes are reset.

- Save changes. Click the **Save** icon.

  Your changes are saved. When the Save icon is grayed out, everything is saved.
- Open the Help screen. Click the **Help** icon.

  The Help pop-up screen displays.
- Enter full-screen mode. Click the **Screen** icon.

  The screen displays in full-screen mode. To return to the regular screen display, either press the **Esc** key, or from the full screen, click the **Screen** icon.
- Print the screen. Click the **Print** icon.

  The topology view is printed.

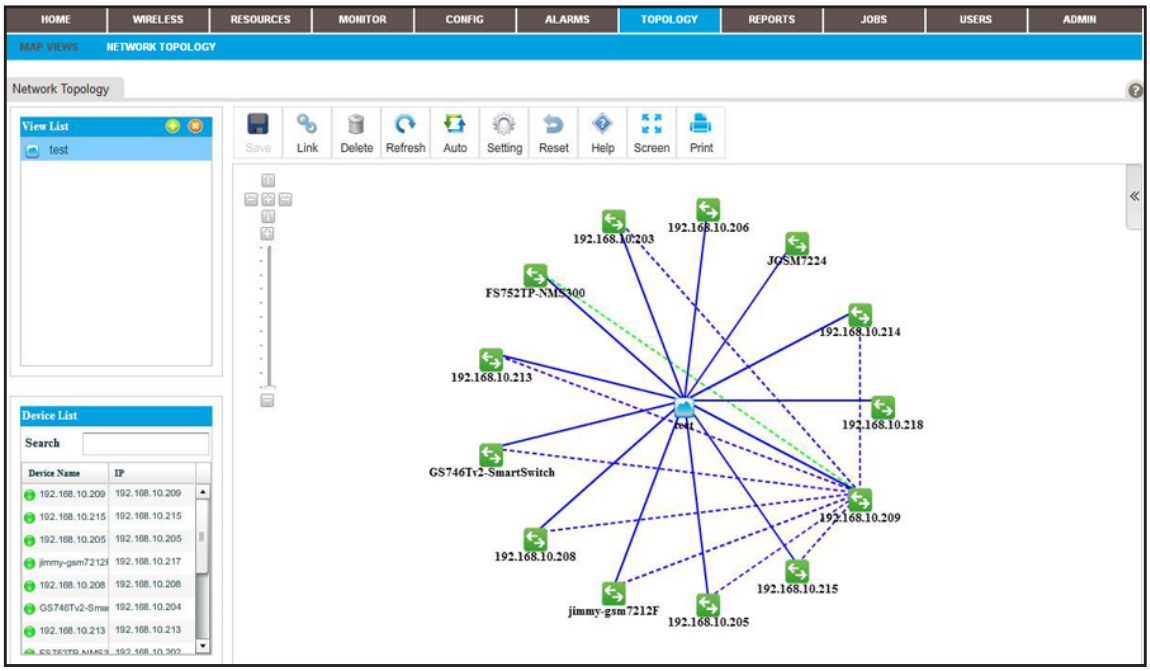
Add a Link Between Devices on a Topology View

You can add a link between devices. For devices that do not support link discovery through Link Layer Discovery Protocol (LLDP), you can manage links manually. When you know that physical connections exist for the non-LLDP devices, you can draw these links manually and also update them manually when the physical connections are reconfigured.

➢ **To add a link between devices on a topology view:**

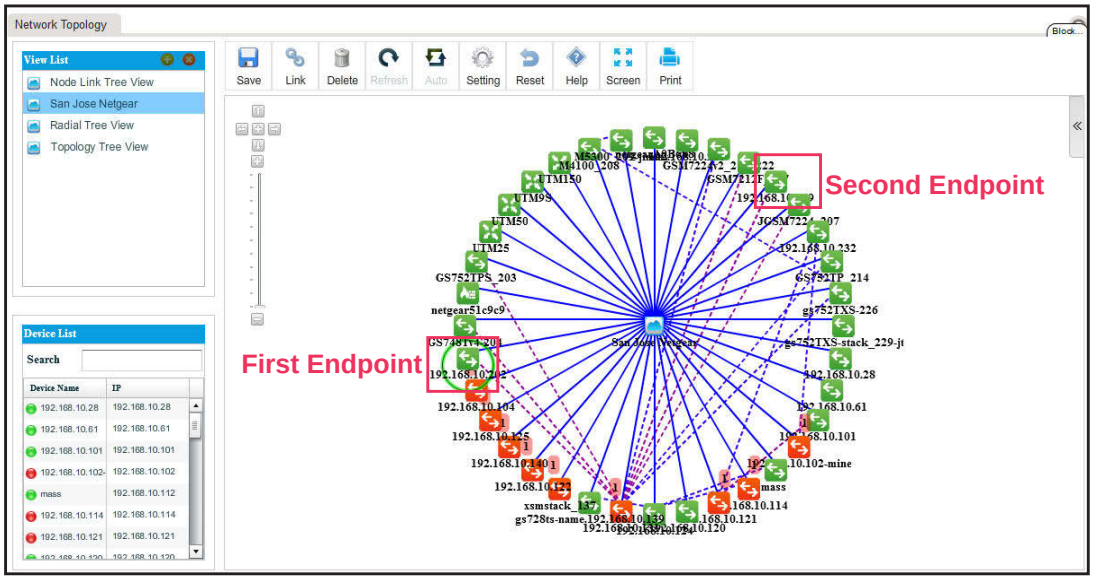
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.
2. Select **TOPOLOGY > NETWORK TOPOLOGY**.



3. From the View List table, select the topology view.

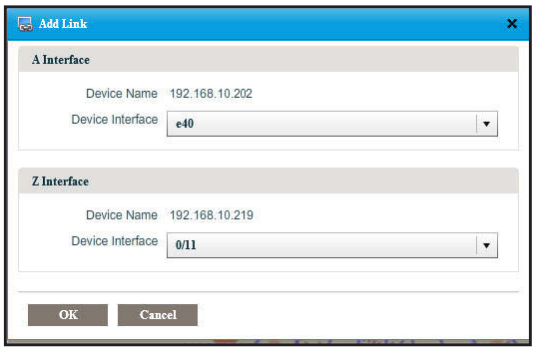
4. Select the device that is the first endpoint of the link:



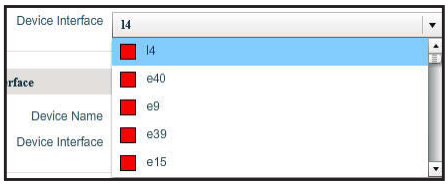
5. Click the **Link** icon.

6. Drag your cursor from the device that you selected in *Step 4* to the device that is the other endpoint of the link.
7. Release the mouse button.

   The Add Link screen displays.



8. From the menus, select the device interface for each end of the link.

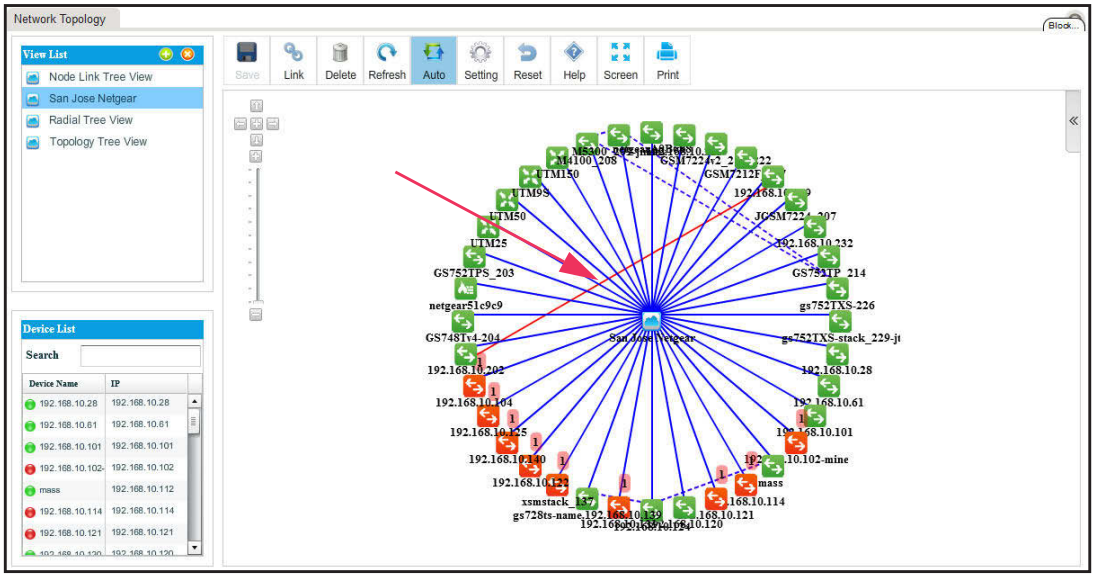


9. Click the **OK** button.

   The Add Link screen closes.

10. Click the **Save** button.

    The link is added between the two devices.



Customize the Style of a Node and Link on a Topology View

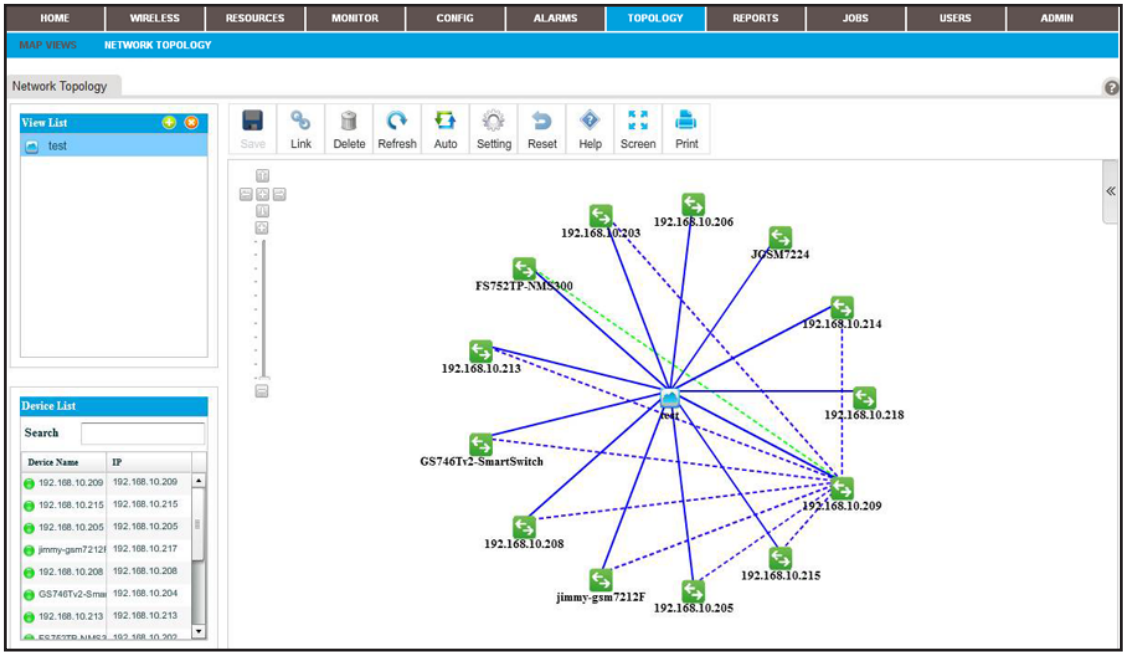
You can customize the way that a node and a link display.

➢ **To customize the style of a node and link:**

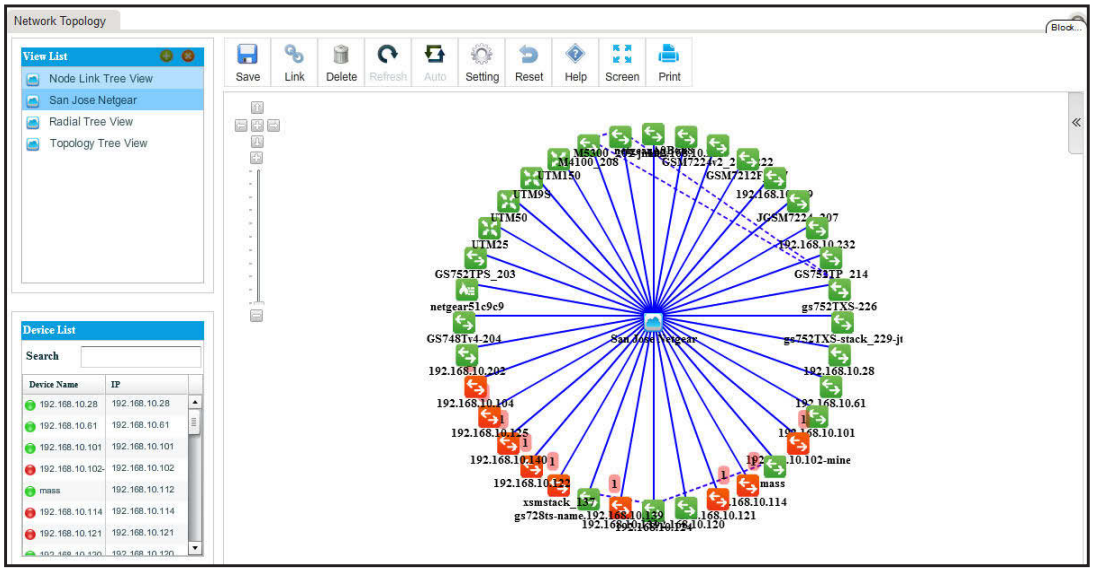
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > NETWORK TOPOLOGY**.

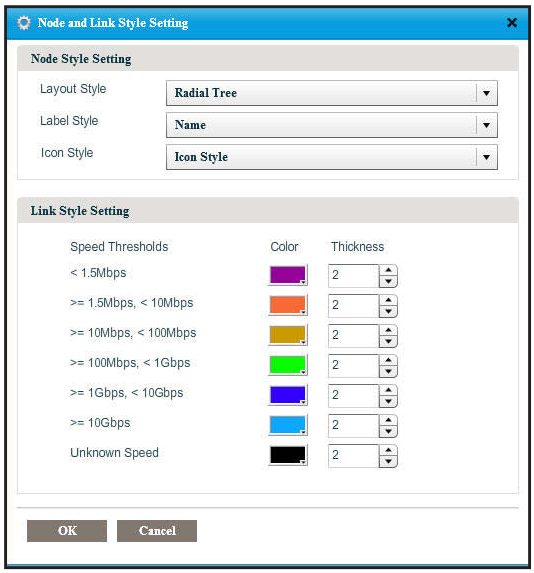


3. From the View List table, select the topology view.

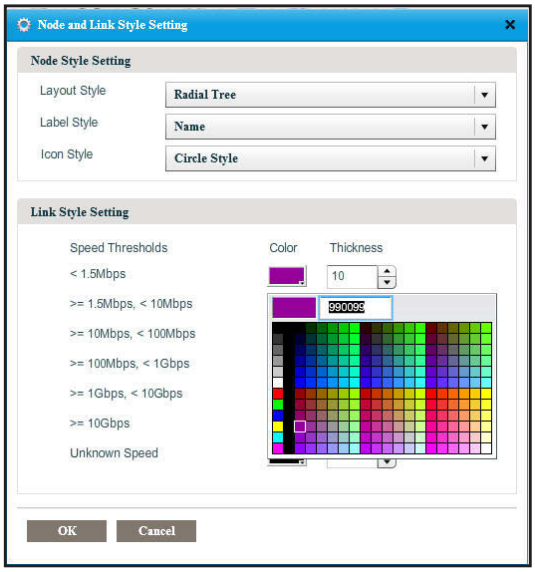


4. Click the **Setting** icon.

The Node and Link Style Settings screen displays.

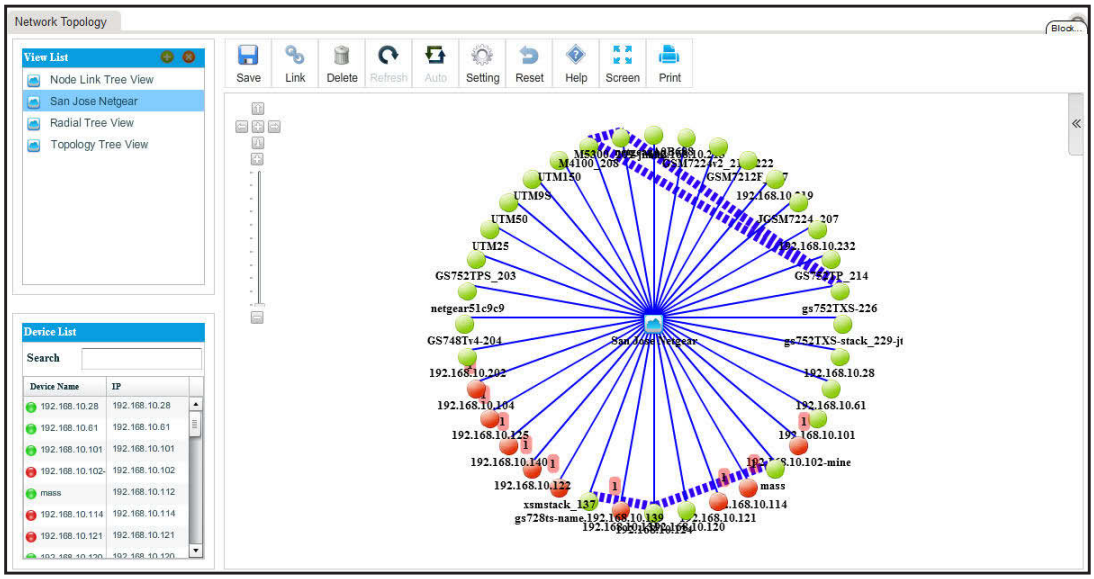


5. Select the node style settings and link style settings:



6. Click the **OK** button.

   The nodes and links on the view display the modified node and link styles.



7. Click the **Save** button.

   Your changes are saved.

Remove a Topology View

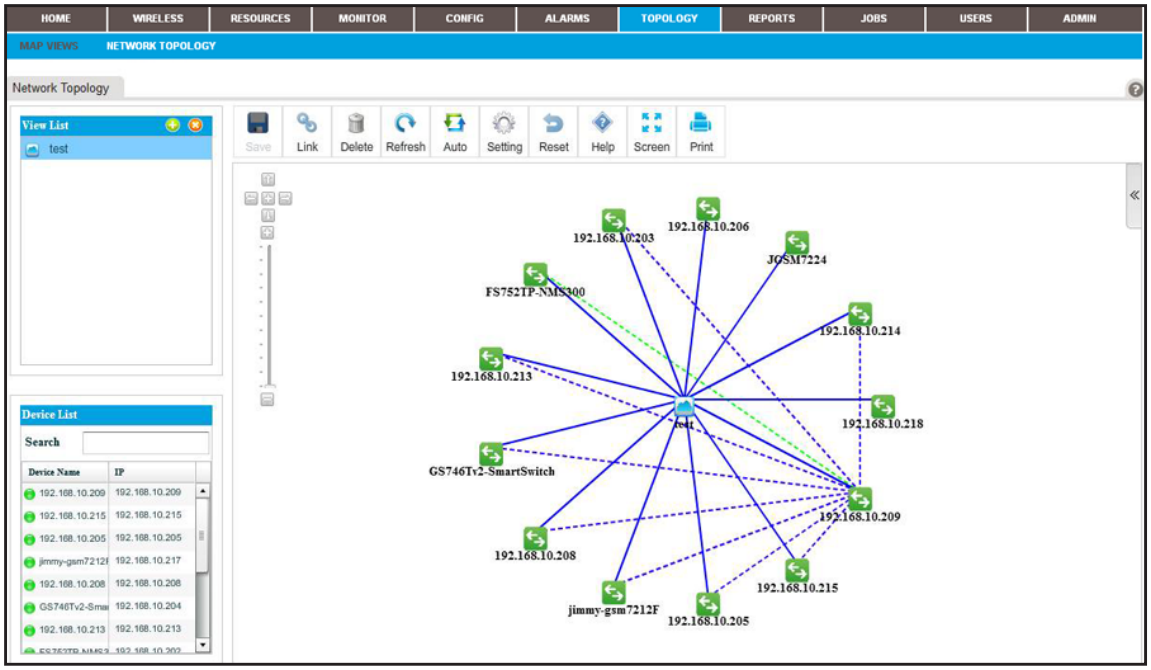
You can remove a topology view that you no longer need.

➢ **To remove a topology view:**

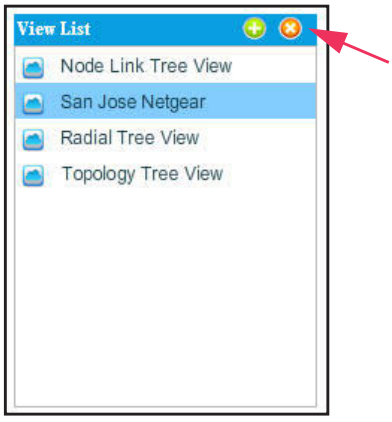
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **TOPOLOGY > NETWORK TOLOPOGY**.



3. From the View List table, select the topology view.
4. Next to View List, click the **X** button.



   A pop-up confirmation screen displays.

5. Click the **Yes** button.

   The topology view is removed from the View List table and deleted.

Generate and View Reports

8

Record how your network performs

You can generate reports from either built-in or customized report templates, and you can view them at any time. You can create new report templates that generate one-time reports or regular reports automatically on a schedule.

This chapter covers the following topics:

- *Manage Report Templates*
- *Generate and Schedule Reports*
- *View and Remove Saved Reports*

Manage Report Templates

The application provides default report templates that are based on inventory, devices, wireless devices, wireless clients, and traffic. You can generate and view a report based on such templates. You can also add a new report template based on an existing template, modify an existing template, and remove a report template.

The following figure shows the types of reports that the templates are based on.

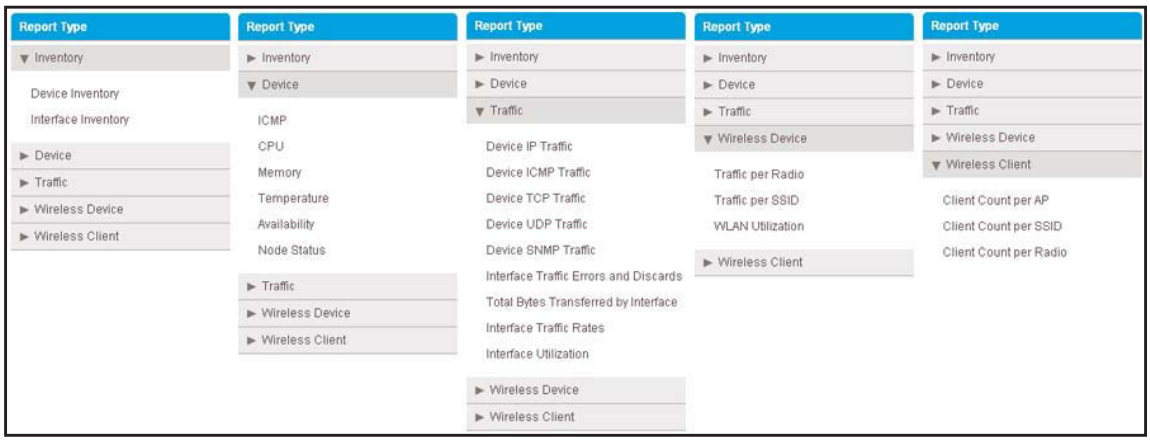


Figure 6. Overview of the types of reports

Add or Modify a Report Template

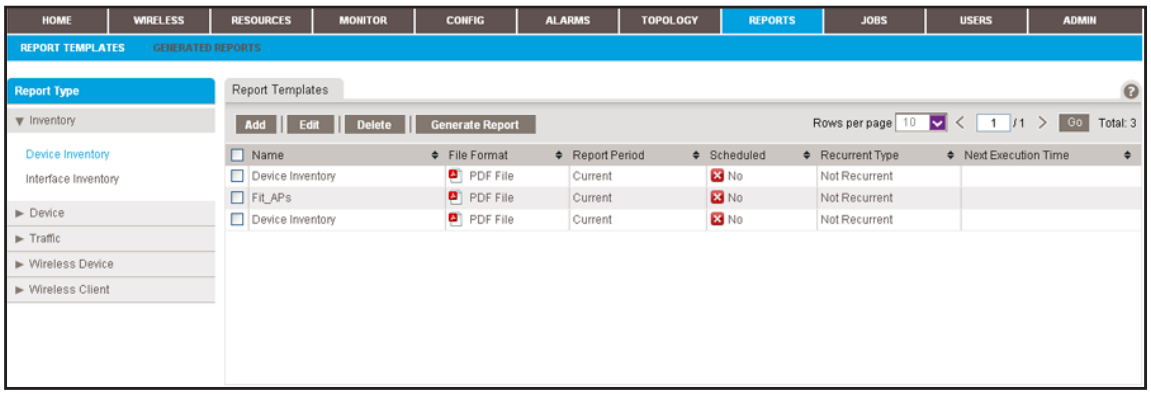
To generate reports for your particular network and situation, you can add a report template that is based on a default report template or modify a default report template.

➢ **To select a report style and add a report template or modify an existing report template:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **REPORTS > REPORT TEMPLATES**.



3. To add columns to or remove them from the Report Templates table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

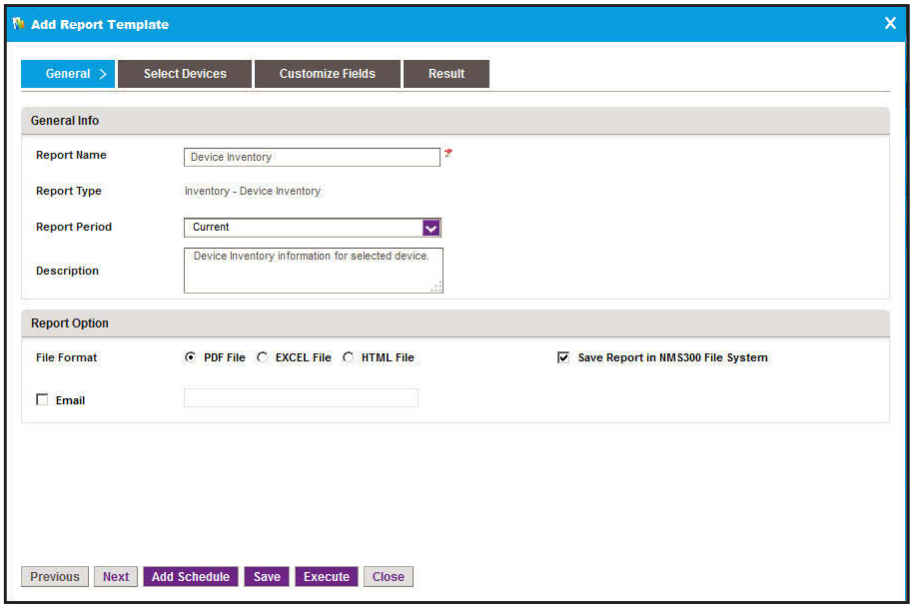
   You can choose from the following columns: Name, File Format, Report Period, Scheduled, Recurrent Type, Next Execution Time, Email, and Description.

4. From the **Report Type** menu, select the report type.

   For some report types, the application provides one or more default report templates. For other report types, the application does not provide any default report templates and you must add a report template.

5. Add a report template or modify an existing report template:
   - To add a report template, click the **Add** button.
   - To modify an existing report template:
     a. From the Report Templates table, select the report template.
     b. Click the **Edit** button.

   For a new report template, the Add Report Template screen displays. For an existing report template, the Edit Report Template screen displays.



   Depending on your type of report selection, a different Add Report Template screen or Edit Report Template screen might display.

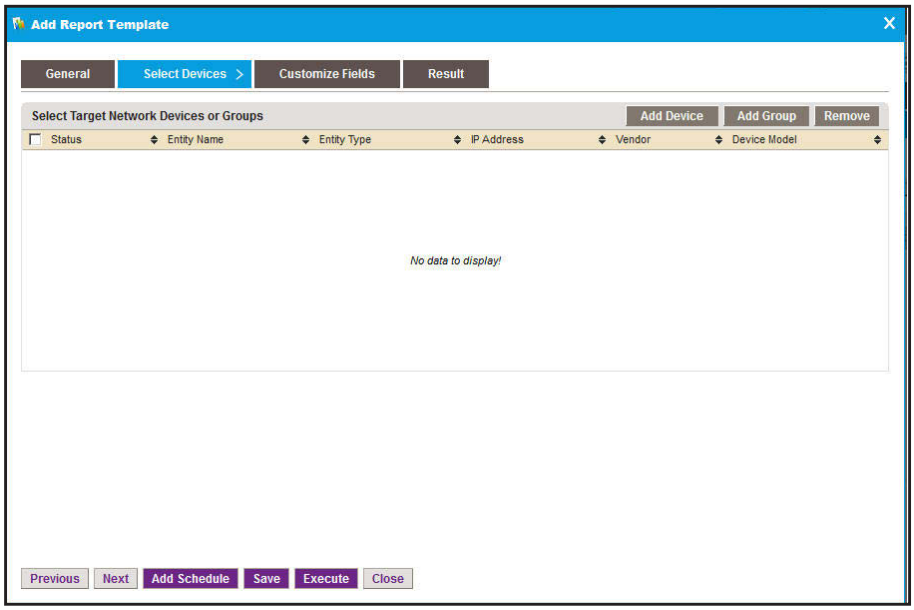
6. Enter or modify the following general report information:
   - **General Info**:
     - **Report Name**. Enter or modify the name for the report template.
     - **Report Type**. Your selection in *Step 4* determines the content of this field.
     - **Report Period**. Select the period to which the report template applies.
     - **Description**. Enter or modify the description for the report template.

- **Report Option**:
  - **File Format**. Select the **PDF File**, **EXCEL File**, or **HTML file** radio button.

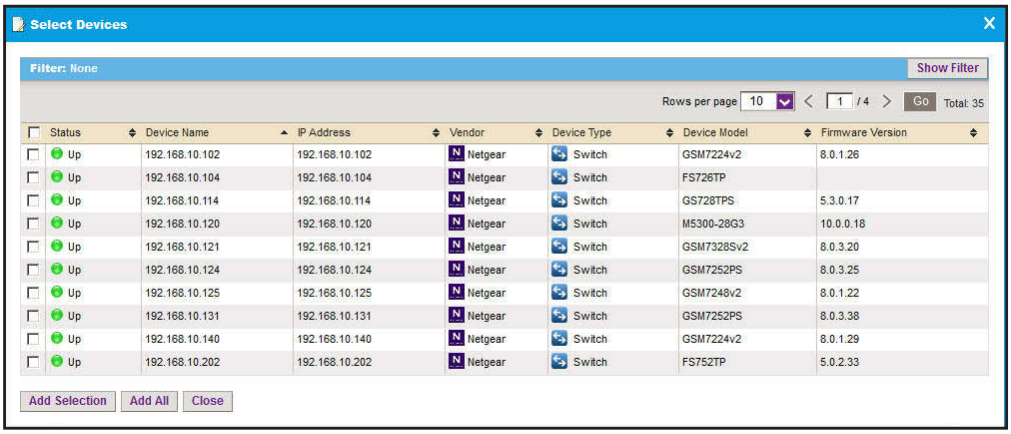
    To save generated reports, select the **Save Reports in NMS300 File System** check box.

    For information about how to view reports that have been generated previously, see *View and Remove Saved Reports* on page 198.
  - **Email**. To have a copy of the report sent to your email address, select the **Email** check box and enter or modify your email address.

7. Click the **Select Devices** tab.



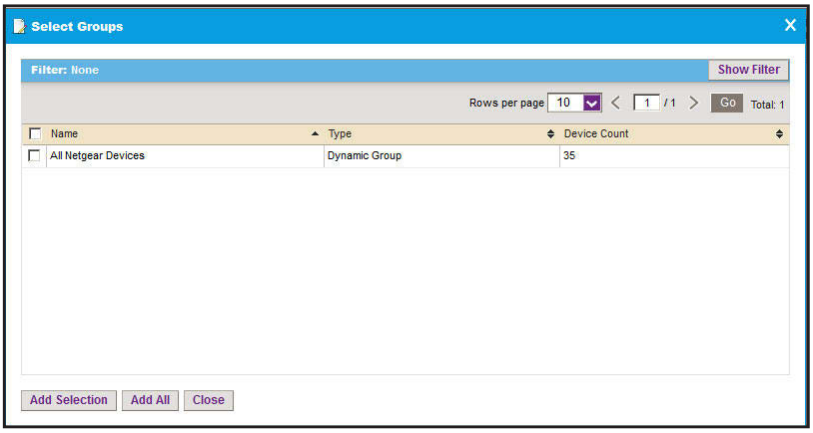
8. Add devices, device groups, or both:
   a. Click the **Add Device** button.



   b. Select devices to add and click the **Add Selection** button.

      To add all of the devices in the table, click the **Add All** button.

c. Click the **Add Group** button.



d. Select device groups to add and click the **Add Selection** button.

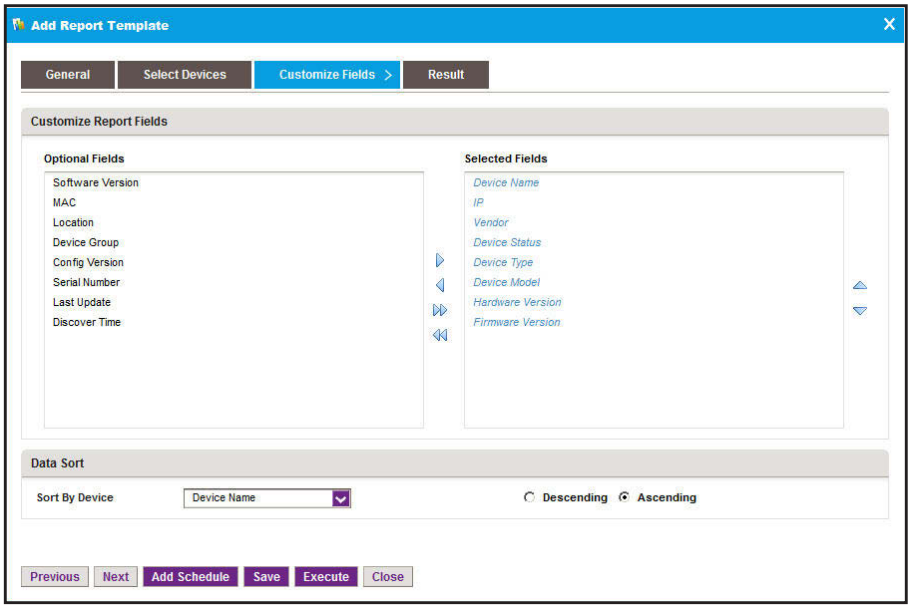
To add all of the device groups in the table, click the **Add All** button.

The selected devices, groups, or both, display in the Select Target Network Devices or Groups table.

e. If you are modifying an existing report template, to remove devices or groups, select the devices or groups, and click the **Remove** button.

The devices or groups are removed from the Select Target Network Devices or Groups table.

9. Click the **Customize Fields** tab.



Depending on your type of report selection, a different Customize Fields screen might display.

a. In the Customize Report Fields section, specify the fields and the order in which you want them to appear in your report template.

   To select the fields, use the **>**, **<**, **>>**, and **<<** buttons. To arrange their order, use the up and down buttons.

b. In the Data Sort section, specify how you want the information sorted.

   You can sort by device and by descending or ascending order.

10. Click the **Save** button.

    The report template is saved and added to the Report Template table.

Remove a Report Template

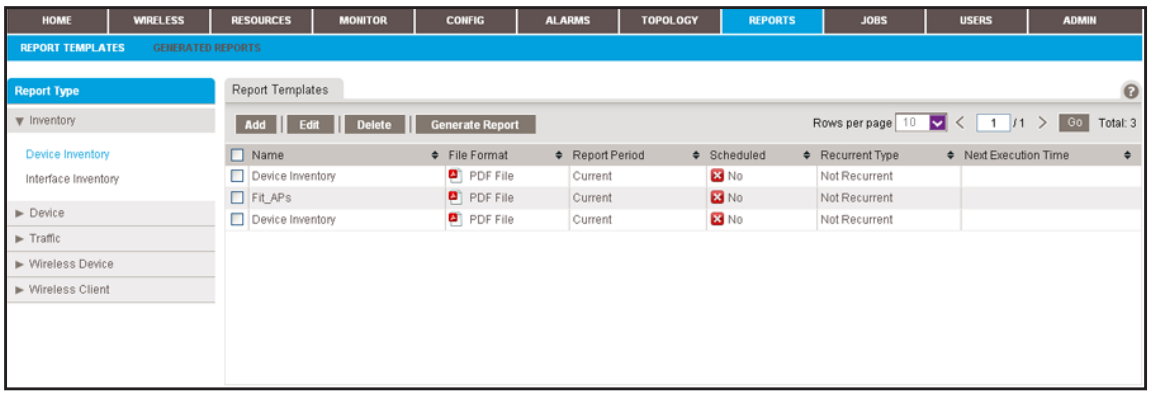
When you delete a report generation job from the Jobs table, the application deletes the report template for the job automatically. For more information, see *View and Manage Jobs* on page 202. You can also remove a report template manually.

➢ **To remove a report template manually:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **REPORTS > REPORT TEMPLATES**.



3. To add columns to or remove them from the Report Templates table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Name, File Format, Report Period, Scheduled, Recurrent Type, Next Execution Time, Email, and Description.

4. From the **Report Type** menu, select the report type.
5. Select the report template.
6. Click the **Delete** button.

   A pop-up confirmation screen displays.

7. Click the **Yes** button.

   The report template is removed from the Report Templates table and deleted.

Generate and Schedule Reports

You can generate reports from an existing report template. You can create one-time reports manually that are generated immediately or schedule one-time reports that are generated later. You can also schedule recurring reports that are generated automatically.

Generate a One-Time Report Immediately

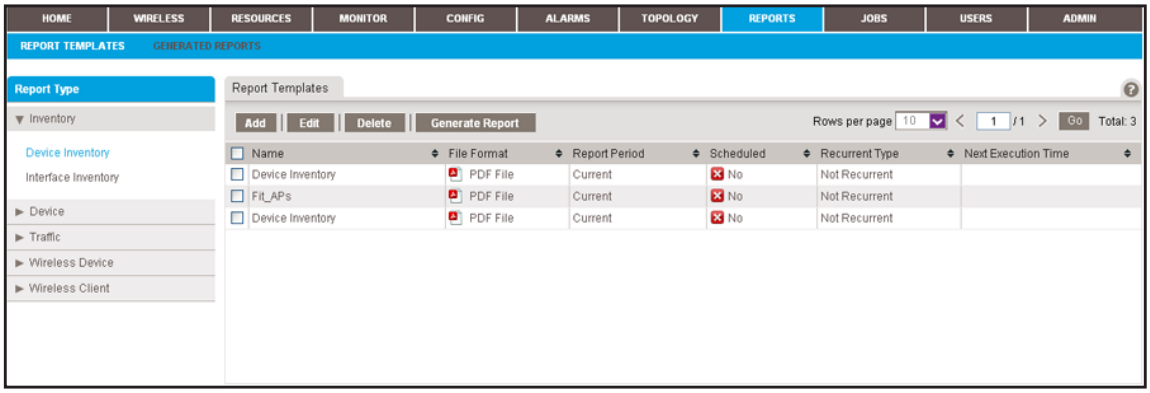
You can generate a new report immediately from an existing template. For information about how to schedule the generation of a one-time report later, see *Schedule a Report* on page 196.

➢ **To generate and view a report:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **REPORTS > REPORT TEMPLATES**.

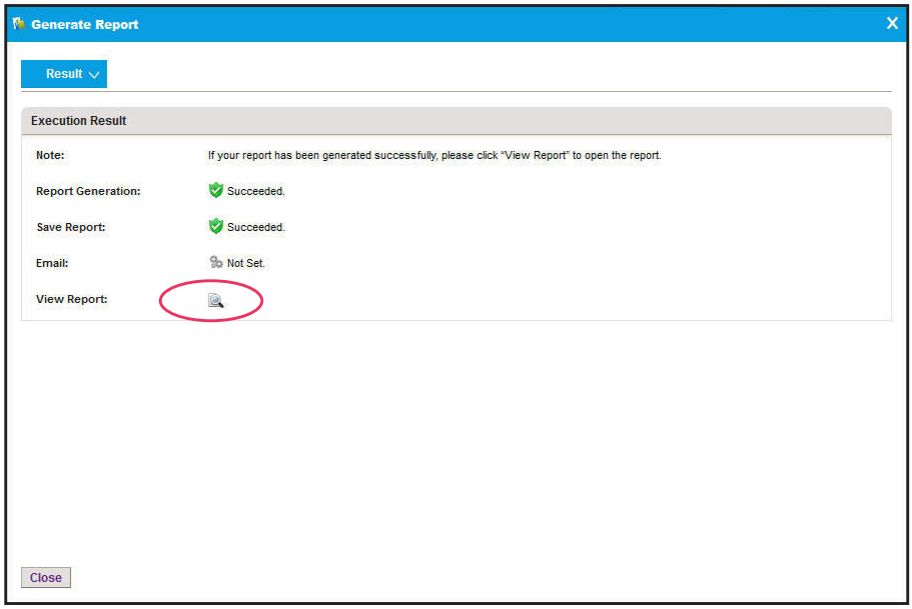


3. To add columns to or remove them from the Report Templates table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Name, File Format, Report Period, Scheduled, Recurrent Type, Next Execution Time, Email, and Description.

4. From the **Report Type** menu, select the report type.
5. Select the report template.
6. Click the **Generate Report** button.

The Generate Report screen displays the results.



7. Click the **View Report** button.

   The report displays.

8. Click the **Close** button.

   The screen closes.

Schedule a Report

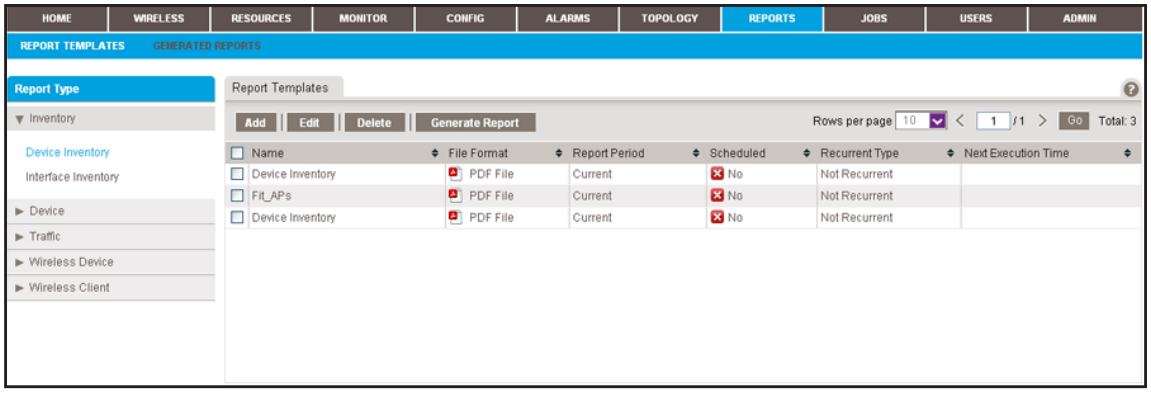
You can schedule a report from an existing template for generation at a future time, or you can schedule the report for generation on a recurring basis.

➢ **To generate a report according to a schedule:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

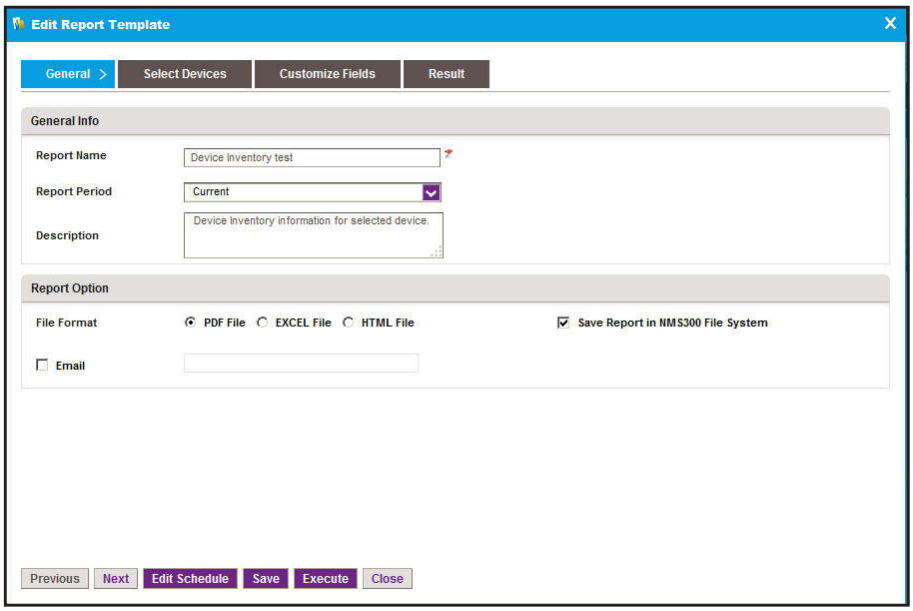
2. Select **REPORTS > REPORT TEMPLATES**.



3. To add columns to or remove them from the Report Templates table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

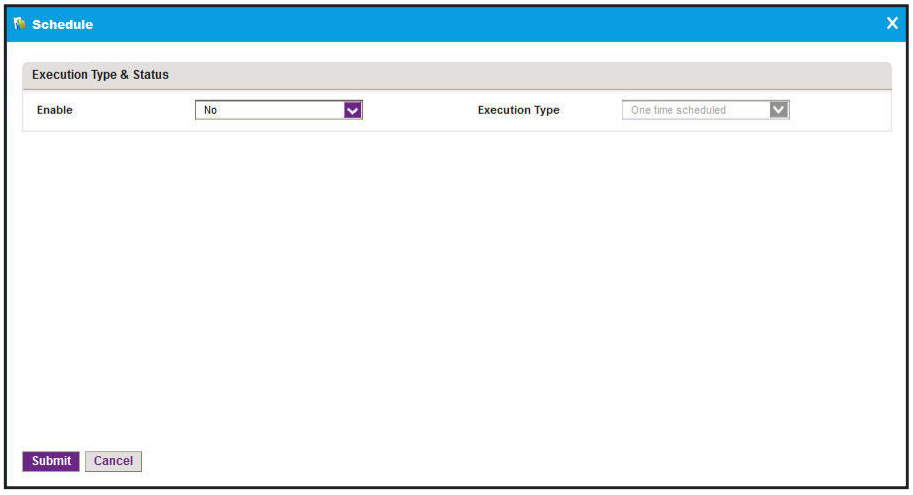
   You can choose from the following columns: Name, File Format, Report Period, Scheduled, Recurrent Type, Next Execution Time, Email, and Description.

4. From the **Report Type** menu, select the report type.
5. Select the report template.
6. Click the **Edit** button.



Depending on your type of report selection, a different Edit Report Template screen might display.

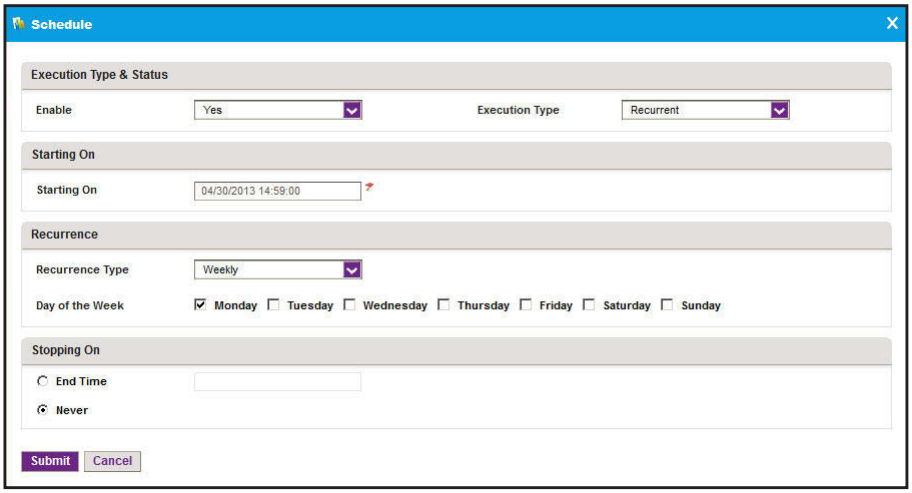
7. Click the **Add Schedule** button.



8. From the **Enable** menu, select **Yes**.

9. Specify whether the application generates the report once or on a recurring basis by selecting one of the following options from the **Execution Type** menu and entering the corresponding information:
   - **One time scheduled**. This is the default selection.

     In the **Starting On** field, enter a date and time.
   - **Recurrent**. The screen adjusts to display more fields.



   Enter the following information:

   a. In the **Starting On** field, enter a date and time.
   b. From the **Recurrence Type** menu, select how the schedule recurs and complete the corresponding field or select the corresponding check boxes.
   c. Select the **End Time** radio button and enter the date and time in the corresponding field, or leave the **Never** radio button selected, which is the default setting.
10. Click the **Submit** button.

    The Schedule screen closes. The report generation schedule becomes part of the report template.
11. On the Edit Report Template screen, click the **Save** button.

    The report is generated according to the schedule that you set.

View and Remove Saved Reports

You can view the saved reports in the application. However, reports are saved for the data retention period. For more information, see *Set the Data Retention Period* on page 214. You can also remove reports that you no longer need.

View a Saved Report

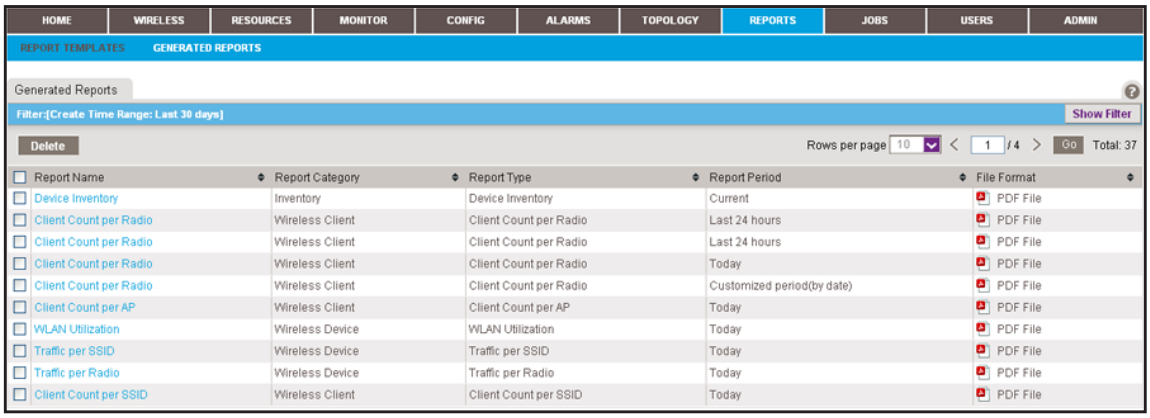
You can view a saved report.

➢ **To view a saved report:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **REPORTS > GENERATED REPORTS**.



3. To add columns to or remove them from the Generated Reports table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Report Name, Report Category, Report Type, Report Period, File Format, Execution Type, Created Time, Created By, and Description.

4. To filter the reports that are listed, click the **Show Filter** button.

   You can filter the current jobs by criteria such as time range, category, and report type. The previous figure shows the Generated Reports table after a time range filter for the past 30 days was applied.

   To hide the filter, click the **Hide Filter** button.

5. Select the report.
6. Double-click the report.

   Your report opens.

Remove a Saved Report

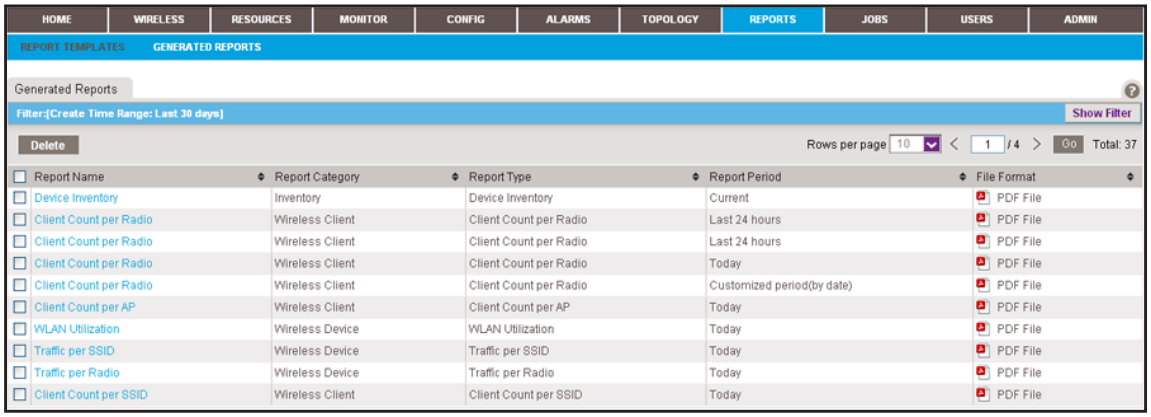
You can remove a saved report that you no longer need.

➢ **To remove a saved report:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **REPORTS > GENERATED REPORTS**.



3. To add columns to or remove them from the Generated Reports table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Report Name, Report Category, Report Type, Report Period, File Format, Execution Type, Created Time, Created By, and Description.

4. To filter the reports that are listed, click the **Show Filter** button.

   You can filter the current jobs by criteria such as time range, category, and report type. The previous figure shows the Generated Reports table after a time range filter for the past 30 days was applied.

   To hide the filter, click the **Hide Filter** button.

5. Select the report.
6. Click the **Delete** button.

   A pop-up confirmation screen displays.

7. Click the **Yes** button.

   The report is removed from the Generated Reports table and deleted.

Manage Jobs

9

Manage the system jobs

You can view job detail and status information.

This chapter covers the following topics:

- *Schedule Jobs*
- *View and Manage Jobs*

Schedule Jobs

The application supports regular and time-consuming jobs that are used for configuration and management tasks. You can schedule these jobs for future execution on a one-time basis or on a recurrent basis for batch operations.

The application supports the following jobs, which are scheduled when you complete the corresponding procedures (see the section references in the following list):

- **Configuration file backup**. Both one-time and recurrent jobs are supported. For more information, see *Schedule a Backup Job* on page 105.
- **Configuration file restore**. One-time jobs are supported. For more information, see *Restore the Configuration of a Single Device* on page 111 and *Restore the Configuration of Several Identical Devices* on page 120.
- **Firmware upgrade**. One-time jobs are supported. For more information, see *Execute or Schedule a Firmware Upgrade* on page 133.
- **Report generation**. Both one-time and recurrent jobs are supported. For more information, see *Schedule a Report* on page 196.
- **Resource discovery**. Both one-time and recurrent jobs are supported. For more information, see *Schedule or Reschedule an Existing Discovery Job* on page 35.

Output files from completed jobs are saved for the data retention period. For more information, see *Set the Data Retention Period* on page 214.

View and Manage Jobs

You can view job detail and status information. You can also enable, disable, and delete jobs. For information about modifying or rescheduling jobs, see the section references in the previous section, *Schedule Jobs*.

When you delete any of the following items from the Jobs table, the application deletes its corresponding profile or template from its database:

- **Discovery job**. You can create a discovery profile. For more information, see *Add or Modify a Discovery Profile* on page 30.
- **Backup job**. You can create a new backup profile. For more information, see *Add or Modify a Backup Profile* on page 101.
- **Report generation job**. You can create a report template. For more information, see *Manage Report Templates* on page 190.

When you delete any of the following items from the Jobs table, the application does *not* delete the related file from its database:

- **Restore configuration job**. To remove the configuration file from the application, you must delete the configuration file manually. For more information, see *Restore Your Device Configurations* on page 110.

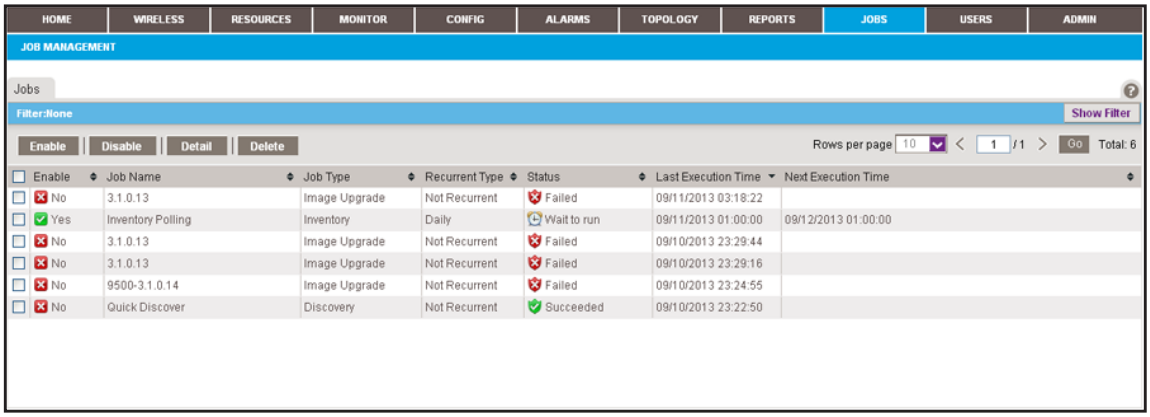
- **Firmware upgrade job**. To remove the firmware file from the application, you must delete the firmware file manually. For more information, see *Upgrade Firmware for One or More Devices* on page 131.

➢ **To view and manage jobs:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **JOBS > JOB MANAGEMENT**.



3. To add columns to or remove them from the Jobs table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Enable, Job Name, Job Type, Recurrent Type, Status, Last Execution Time, Next Execution Time, Last Execution Status, Job End Time, Created By, and Create Time.

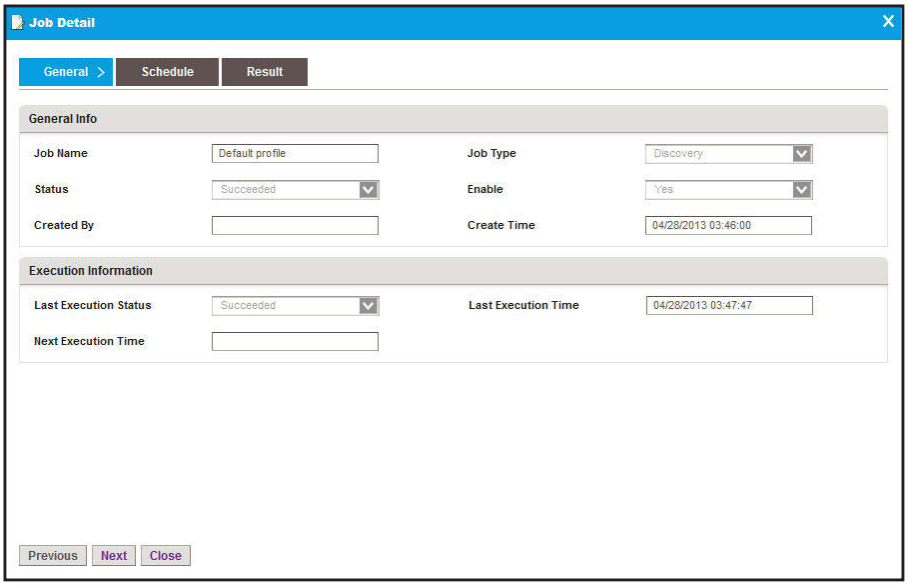
4. To filter the jobs that are listed, click the **Show Filter** button.

   You can filter the current jobs by criteria such as job type, status, and last execution time.

   To hide the filter, click the **Hide Filter** button.

5. Select a job.
6. Take one of the following actions:
   - Enable the job. Click the **Enable** button.
   - Disable the job. Click the **Disable** button.

- Display job details. Click the **Detail** button.



  Depending on your selection, a different Job Detail screen might display.

  To close the Job Detail screen, click the **Close** button.

- Delete the job:

  a. Click the **Delete** button.

  A pop-up confirmation screen displays.

  b. Click the **Yes** button.

  The job is removed from the Jobs table and deleted.

Manage Users and Security Profiles 10

Manage the system users

You can manage security profiles, the user base, and online users.

This chapter covers the following topics:

- *Security Profile Concepts*
- *Add a Security Profile*
- *Modify or Remove a Security Profile*
- *Add a User Profile to the User Base*
- *Modify or Remove a User Profile*
- *View and Log Off Online Users*

Note: Only admin users (that is, users with a security profile that is set to Admin) can perform user management tasks.

Security Profile Concepts

The application provides the following default user security profiles:

- **Admin**. A user who can perform *all* functions of the application, including management of users and security profiles.
- **Operator**. A user who can manage the network functions, but cannot manage users or security profiles, or perform administrative tasks.
- **Observer**. A user who can only monitor and view network functions.

As an admin user, you can modify and delete these security profiles and you can define new security profiles. For example, you can add a security profile for someone who can only run and view network reports but is not authorized to perform any other tasks.

Add a Security Profile

If one of the default security profiles does not satisfy your needs, you can add a security profile and specify the tasks that are associated with the security profile. For most functions, you can specify whether the security profile includes viewing only, modifying only, or both viewing and modifying. You can specify the following tasks in a security profile:

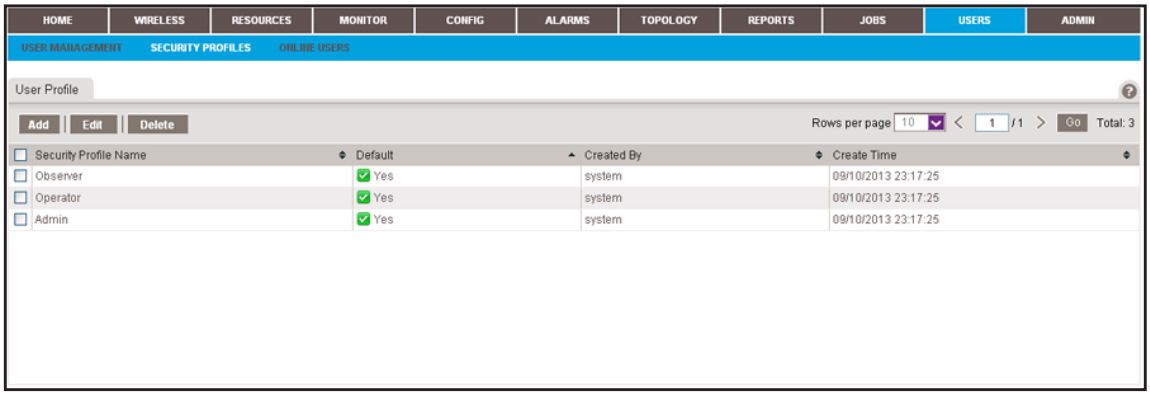
- Monitoring
- Configuring
- Managing alarms
- Managing topologies
- Discovering
- Reporting
- Managing jobs
- Managing users and security profiles
- Performing administrative tasks

➢ **To view the existing security profiles and add a security profile:**

1. Log in to the application.

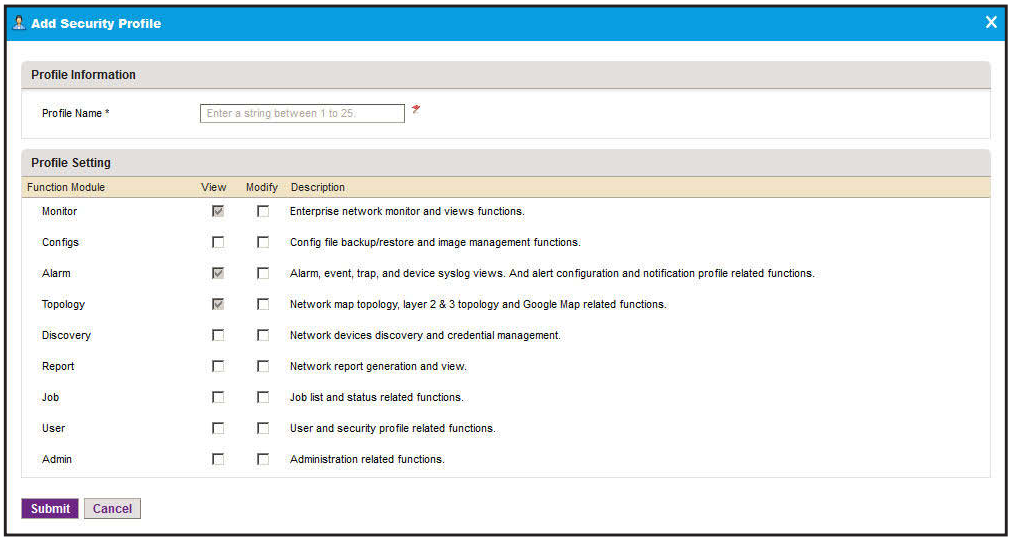
   For more information, see *Log In to the Application* on page 15.

2. Select **USERS > SECURITY PROFILES**.



3. Click the **Add** button.

   The Add Security profile screen displays.



4. In the **Profile Name** field, enter a name.
5. In the Profile settings section of the screen, select the check boxes for the functions that you want to include in the security profile.
6. Click the **Submit** button.

   The security profile is saved and added to the User Profile table.

Modify or Remove a Security Profile

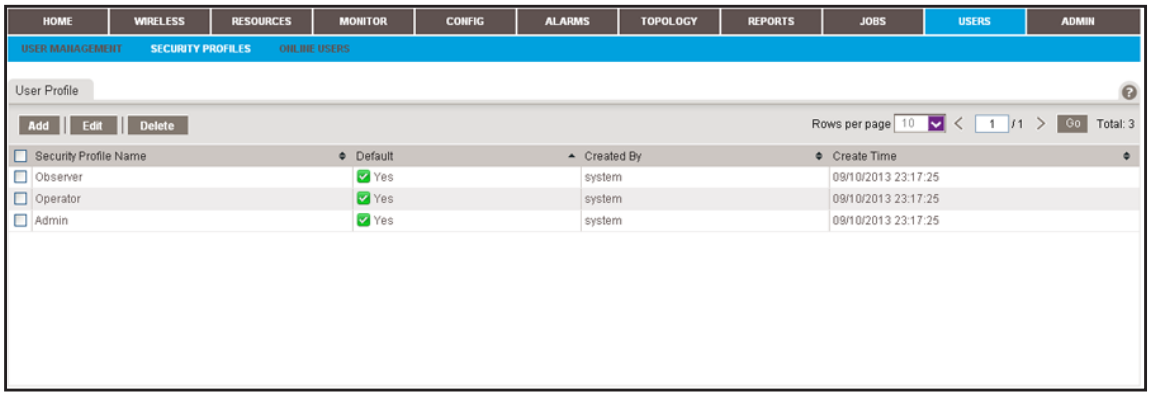
You can modify or remove a security profile. For a default security profile, you can change only the profile name. For a custom security profile, you can change the profile name and the tasks. You cannot remove a default security profile.

➢ **To modify or remove a security profile:**

1. Log in to the application.

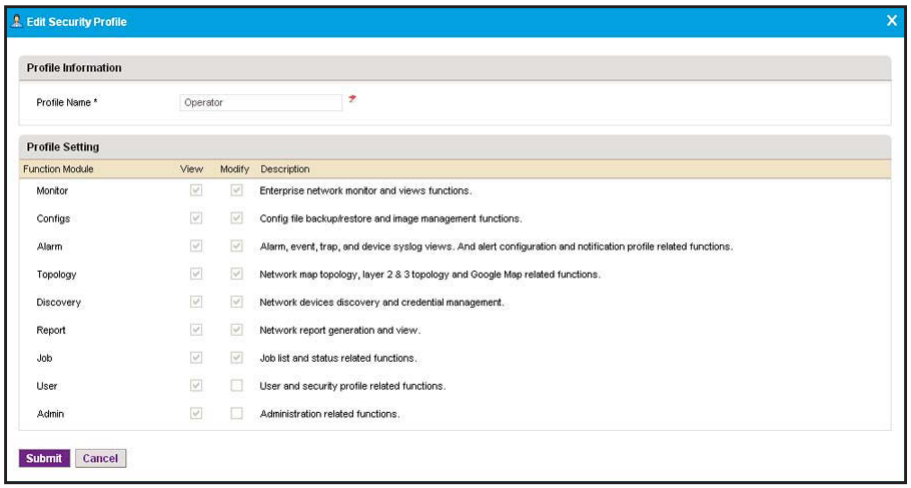
For more information, see *Log In to the Application* on page 15.

2. Select **USERS > SECURITY PROFILES**.



3. Select the security profile.
4. Take one of the following actions:
   - Modify the security profile:
     a. Click the **Edit** button.

        The Edit Security Profile screen displays.



     b. (Optional) In the **Profile Name** field, modify the name.
     c. (Optional) In the Profile settings section of the screen, select the check boxes for the functions that you want to include in the security profile.

        For a default security profile, you can change only the profile name.
     d. Click the **Submit** button.

        The modified security profile is saved and added to the User Profile table.
   - Remove the security profile:
     a. Click the **Delete** button.

        You cannot remove a default security profile.

A pop-up confirmation screen displays.

b. Click the **Yes** button.

The security profile is removed from the User Profile table and deleted.

Add a User Profile to the User Base

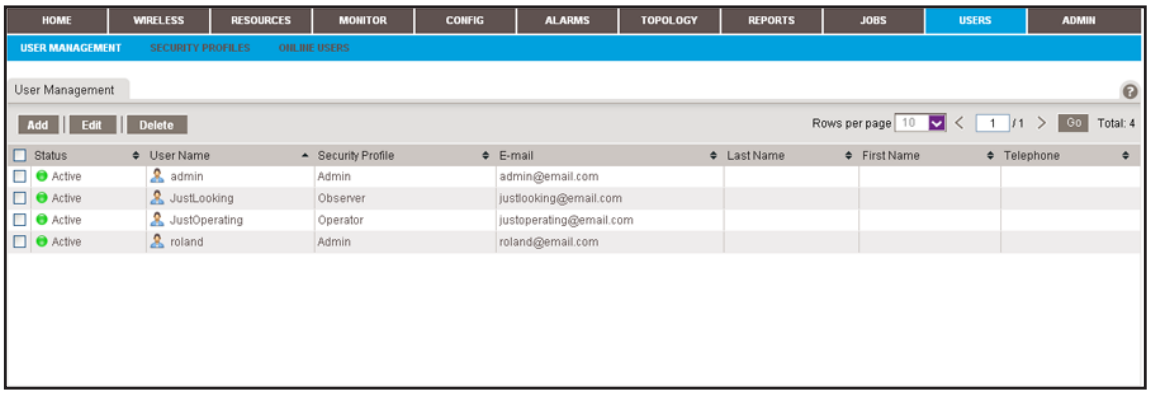
The application has one default user profile, which is a user with the name admin to which an Admin security profile is assigned. You can add multiple user profiles to the user base.

➢ **To view the existing user profiles and add a user profile:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

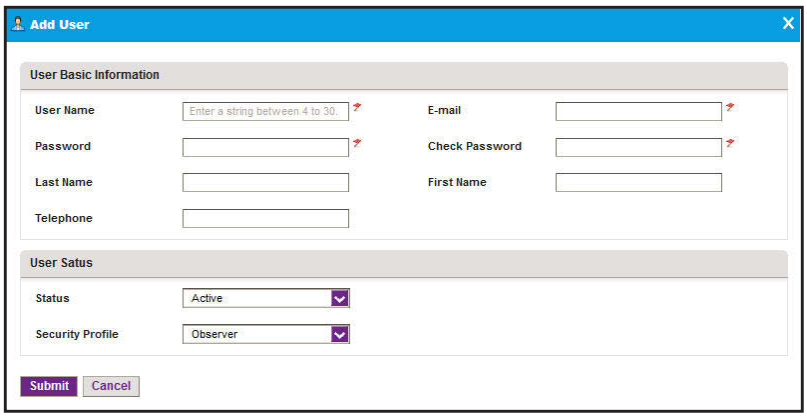
2. Select **USERS > USER MANAGEMENT**.



The Status column displays whether the user is active and can log in.

3. Click the **Add** button.

   The Add User screen displays.



4. Specify the following information:
   - In the User Basic Information section, enter the user name, password, and email address for the user. The first and last name and telephone number are optional.

- In the User Status section, select whether the user profile is active and select the security profile that applies to the user.

For more information about security profiles, see *Security Profile Concepts* on page 206.

5. Click the **Submit** button.

   The screen closes and the new user is added to the User Management table.

Modify or Remove a User Profile

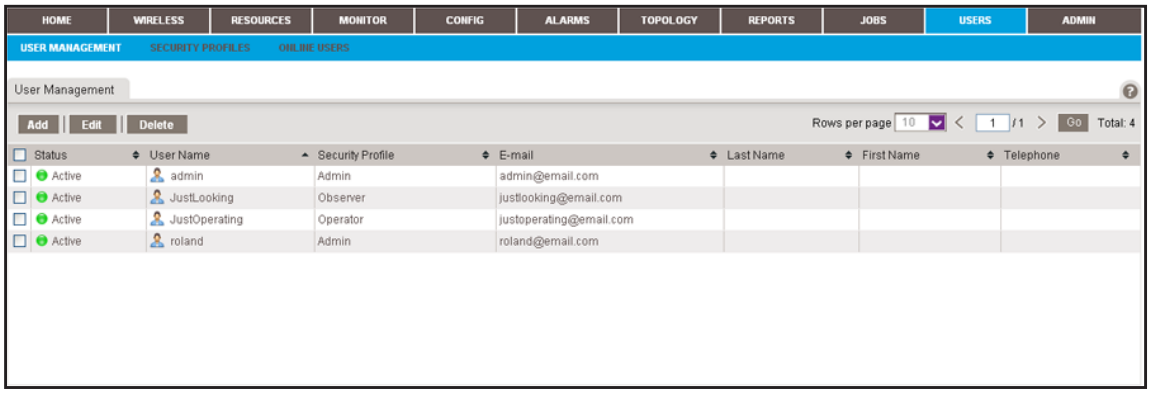
You can modify or remove a user profile.

➢ **To modify or remove a user profile:**

1. Log in to the application.

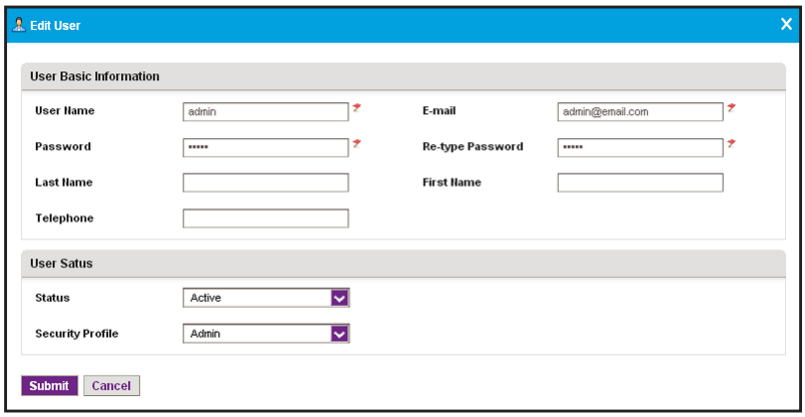
   For more information, see *Log In to the Application* on page 15.

2. Select **USERS > USER MANAGEMENT**.



3. Select the user profile.
4. Take one of the following actions:
   - Modify the user profile:
     a. Click the **Edit** button.

        The Edit User screen displays.



a. (Optional) In the User Basic Information section, modify the user name, password, or email address for the user. The first and last name and telephone number are optional.

b. In the User Status section, select whether the user profile is active and select the security profile that applies to the user.

   For more information about security profiles, see *Security Profile Concepts* on page 206.

c. Click the **Submit** button.

   The modified user profile is saved and added to the User Management table.

- Remove the user profile:

  a. Click the **Delete** button.

     A pop-up confirmation screen displays.

  b. Click the **Yes** button.

     The user profile is removed from the User Management table and deleted.

View and Log Off Online Users

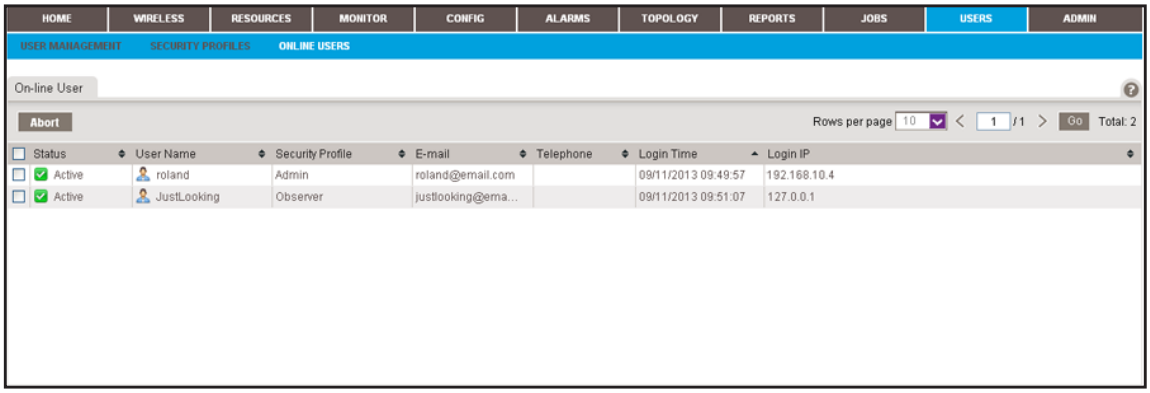
You can view the users who are currently logged in and log them off:

➢ **To view and log off (abort) users who are online:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **USERS > ONLINE USERS**.



3. To add columns to or remove them from the Online User table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: Status, User Name, Security Profile, E-mail, Telephone, Login Time, Login IP, First Name, and Last Name.

4. Select one or more users.

   To select all users, select the check box at the left in the table heading.

5. Click the **Abort** button.

   A pop-up confirmation screen displays.

6. Click the **Yes** button.

   The users are logged off.

11 Customize Global Settings

Customize select global system settings

You can change global settings from the administration dashboard. Except for the procedures that are described in this chapter, all procedures that you can perform from the System and Website Setting screen of the administration dashboard are described in the subject-specific chapters.

This chapter covers the following topics:

- *Set the Data Retention Period*
- *Set the Inventory Polling*
- *Set the Idle Time-Out*
- *Set the Real-time Chart*
- *Change the Auto Refresh Setting*

Note: Only admin users (that is, users with a security profile that is set to Admin) can customize the global settings that are described in this chapter.

Set the Data Retention Period

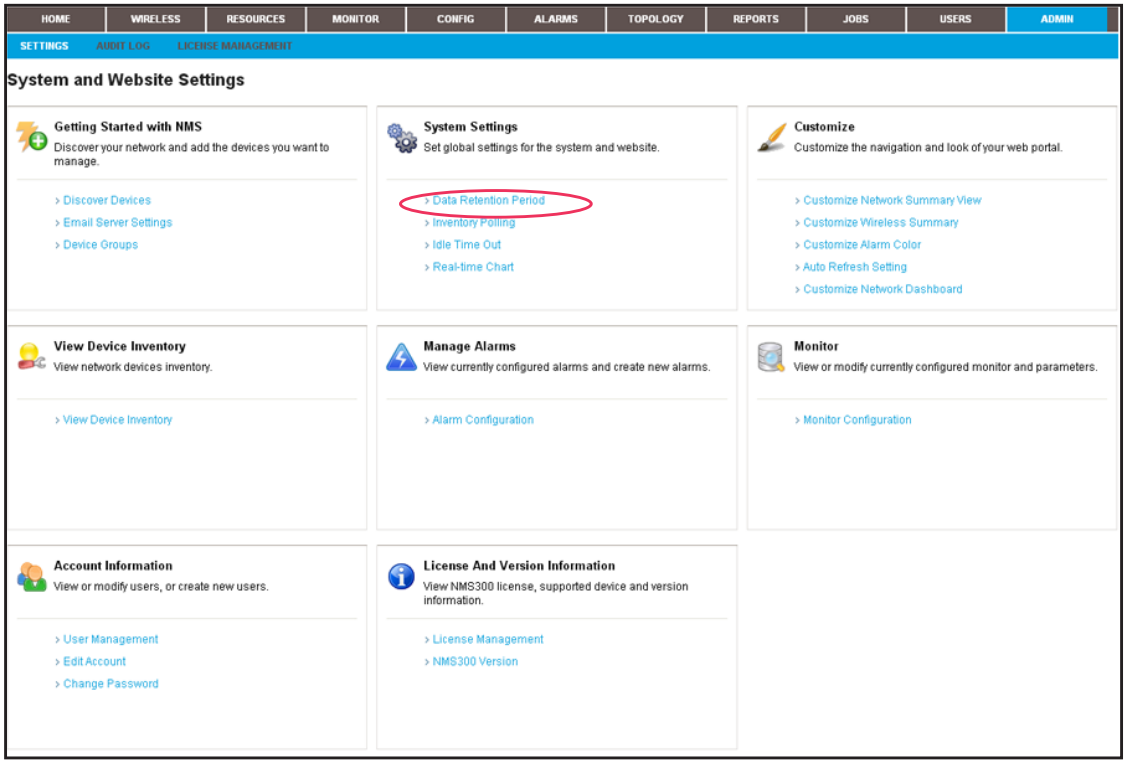
You can change how long the application retains your network data. The longer information is retained, the more disk space is required on the NMS300 server. You can monitor the NMS300 server information (see *View the NMS300 Server Information* on page 97).

➢ **To modify the data retention period:**

1. Log in to the application.

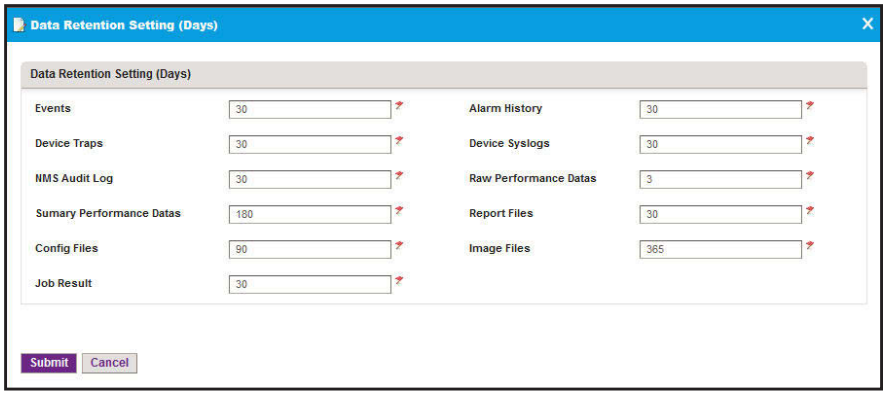
   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under System Settings, click the **Data Retention Period** link.

   The Data Retention Settings screen displays.



4. For the data retention periods that you want to change, enter the updated information:
   - **Events**. This setting determines how long events are retained. The default period is 30 days. For more information, see *View and Manage Network Event Notifications* on page 157.
   - **Device Traps**. This setting determines how long trap data is retained. The default period is 30 days. For more information, see *View and Manage Device Traps* on page 158.
   - **NMS Audit Log**. This setting determines how long audit logs are retained. The default period is 30 days. For more information, see *View and Export Audit Logs* on page 95.
   - **Summary Performance Data**. This setting determines how long summary performance data is retained. The default period is 180 days. For more information, see *Customize the Optional Network Dashboard* on page 88.
   - **Configuration Files**. This setting determines how long backed-up configuration files are retained. The default period is 90 days. For more information, see *Back Up Your Device Configurations* on page 101.
   - **Job Result**. This setting determines how long job execution reports are retained. For more information, see *View and Manage Jobs* on page 202.
   - **Alarm History**. This setting determines how long alarms are retained. The default period is 30 days. For more information, see *View and Manage the Alarm History* on page 144.
   - **Device Syslogs**. This setting determines how long syslogs are retained. The default period is 30 days. For more information, see *View and Manage Device System Logs* on page 160.
   - **Raw Performance Data**. This setting determines how long raw performance data is retained. The default period is 3 days. For more information, see *Manage the Configuration Monitors* on page 83.
   - **Report Files**. This setting determines how long job reports are retained. The default period is 30 days. For more information, see *View and Remove Saved Reports* on page 198.
   - **Image Files**. This setting determines how long device firmware files are retained. The default period is 365 days. For more information, see *Upgrade Firmware for One or More Devices* on page 131.
5. Click the **Submit** button.

   Your changes are saved.

Set the Inventory Polling

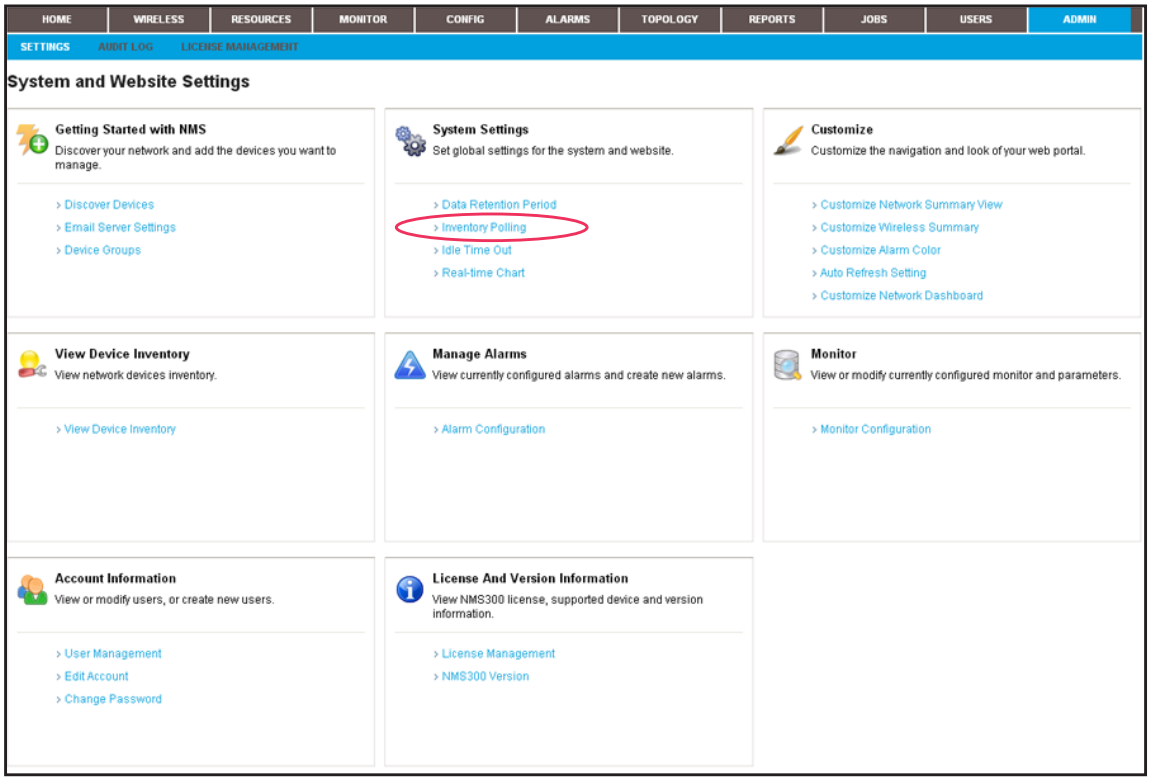
You can change how often the application polls the network for your device inventory.

➢ **To modify the inventory polling:**

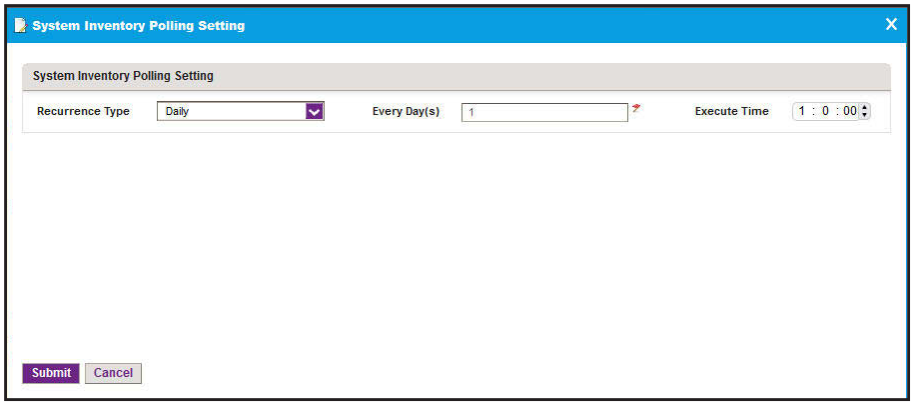
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under System Settings, click the **Inventory Polling** link.



4. Specify the recurrence type and execution time.

   If you select **Hourly** from the **Recurrence Type** menu, the screen adjusts.

5. Click the **Submit** button.

   Your changes are saved.

Set the Idle Time-Out

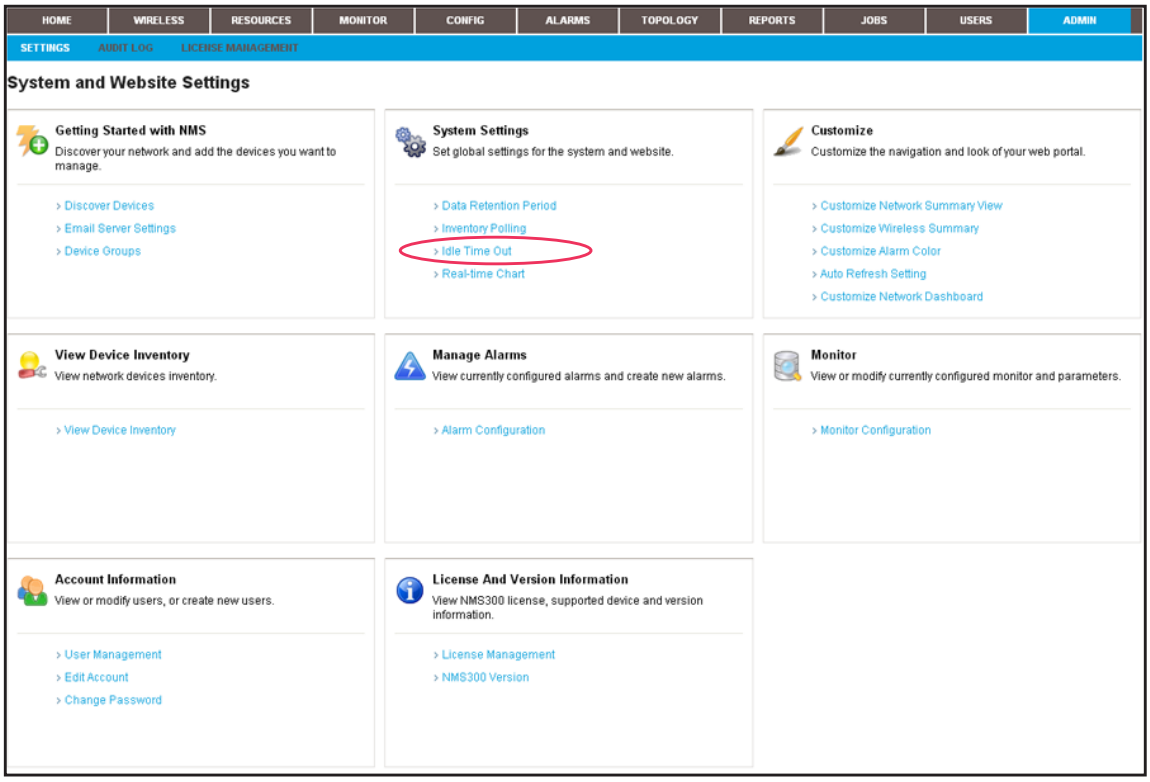
You can change how long the application waits before it logs you out for inactivity. The default period is 30 minutes.

➢ **To modify the idle time-out:**

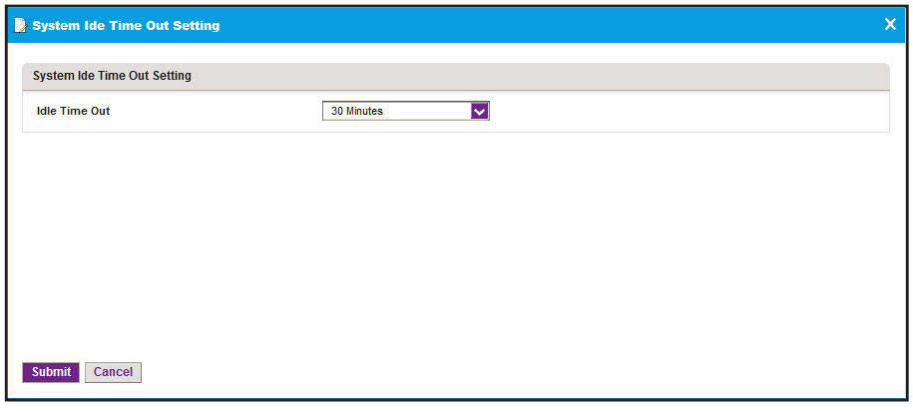
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under System Settings, click the **Idle Time Out** link.



4. Specify the new idle time-out period.

5. Click the **Submit** button.

   Your changes are saved.

Set the Real-time Chart

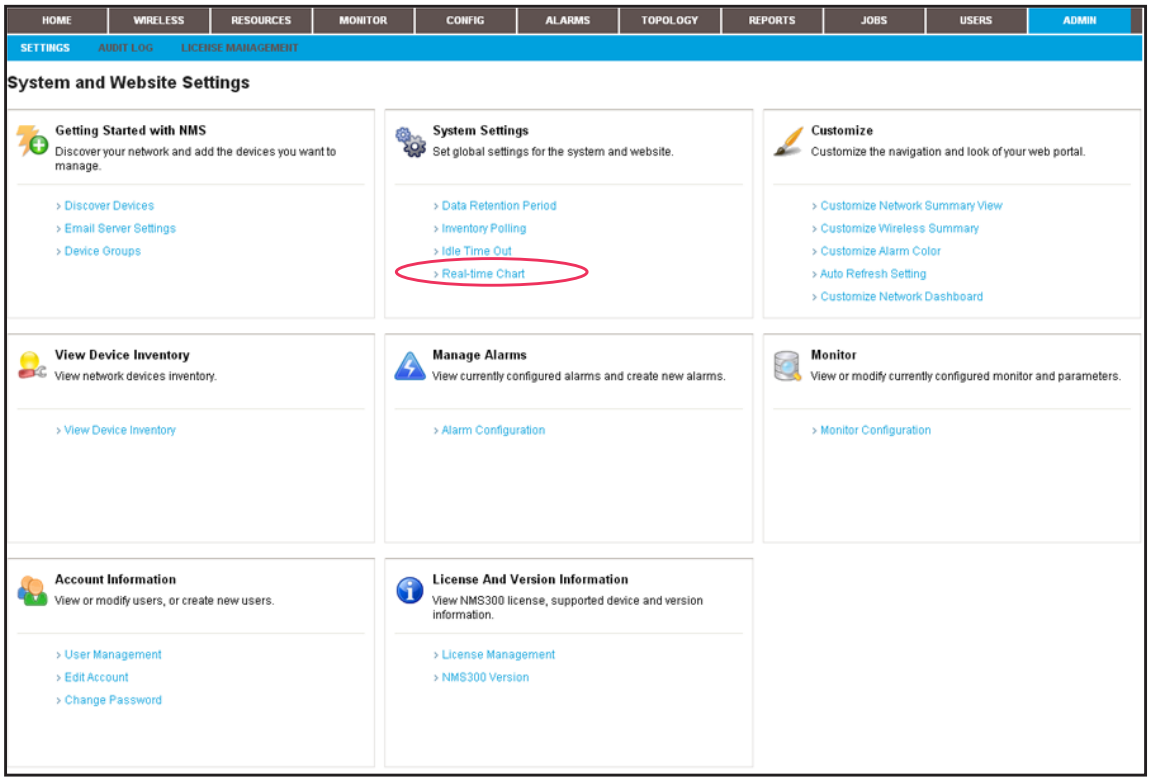
You can change how often the application refreshes your chart data and the maximum time range that is displayed on your charts. By default, the data refresh interval is 10 seconds and the maximum time range is 5 minutes.

➢ **To modify the chart settings:**

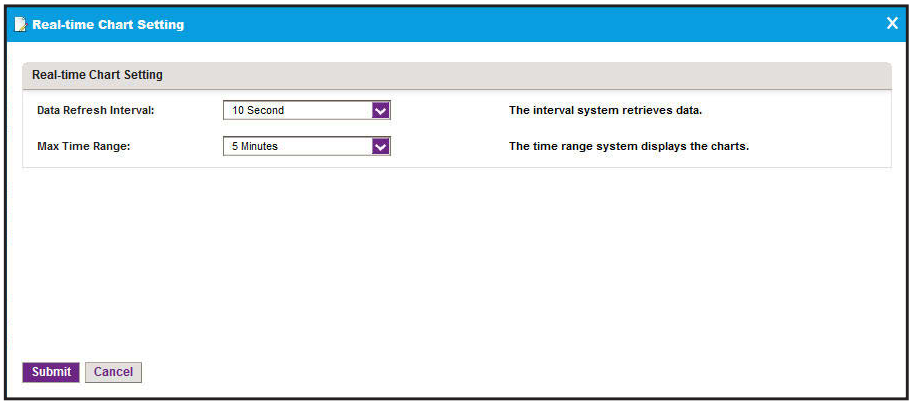
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under System Settings, click the **Real-time Chart** link.



4. Specify the data refresh interval and maximum time range.
5. Click the **Submit** button.

   Your changes are saved.

Change the Auto Refresh Setting

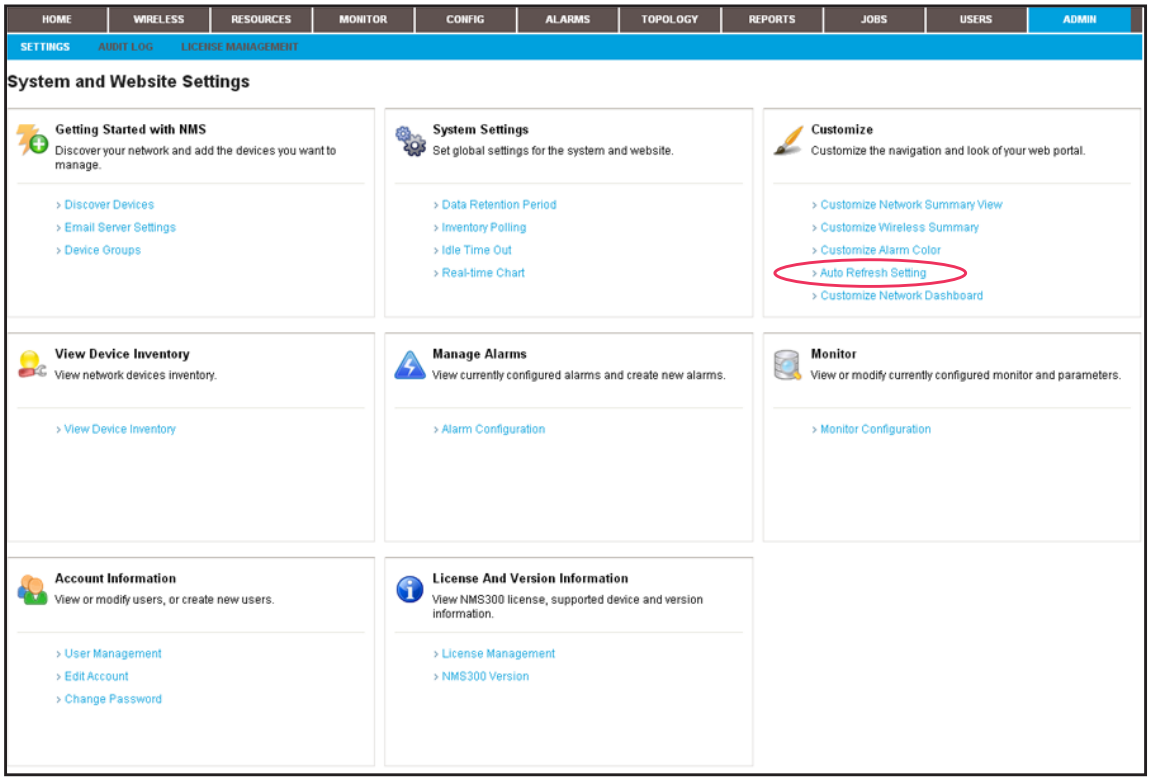
You can change how often the application refreshes the browser screen for the web management interface. By default, the screen refresh interval is one minute.

➢ **To modify the auto refresh settings:**

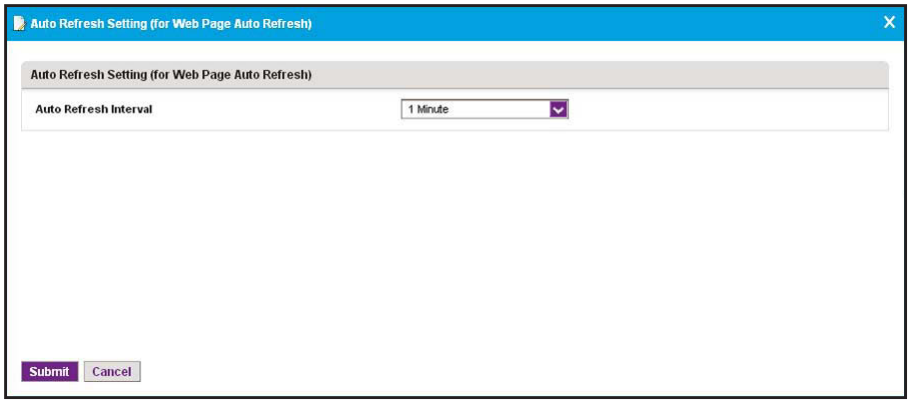
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > SETTINGS**.



3. Under Customize, click the **Auto Refresh Setting** link.



4. Specify the new auto refresh interval.
5. Click the **Submit** button.

   Your changes are saved.

12 Manage Licenses

Manage the system licenses

You can view license information, add a license, and deregister a license.

This chapter covers the following topics:

- *View License Information*
- *Register a License*
- *Deregister a License*

> **Note:** Only admin users (that is, users with a security profile that is set to Admin) can perform license management tasks.

View License Information

The default license that comes with the application supports up to 200 devices. Each device that the application discovers and adds to its device inventory is subtracted from the balance of 200 devices. However, controller-managed APs are not subtracted from the balance.

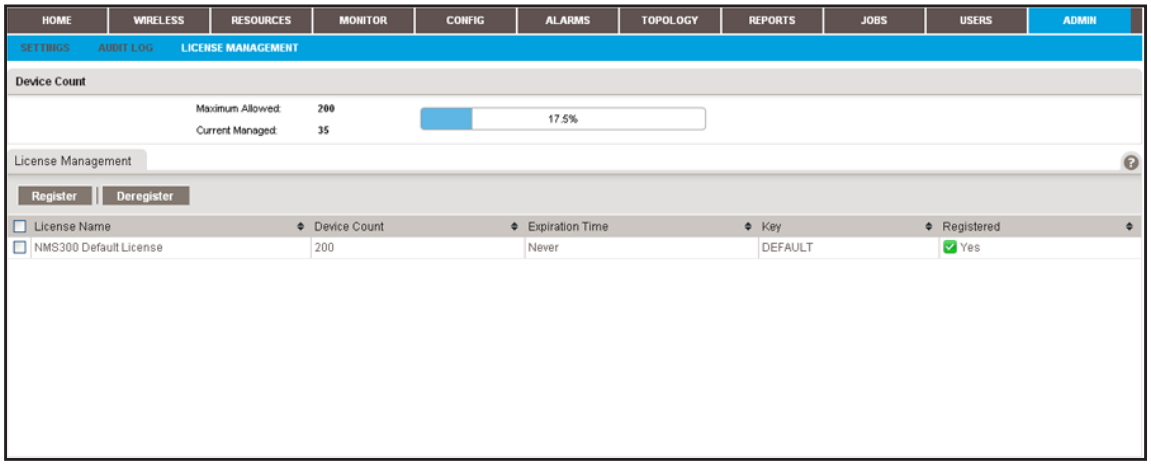
For information about managing more than 200 devices, contact your NETGEAR sales contact.

➢ **To view license information:**

1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > LICENSE MANAGEMENT**.



   The Device Count section of the screen displays the maximum allowed devices with the current license or licenses and the number of devices that the application manages.

3. To add columns to or remove them from the License Management table, right-click the table heading anywhere, and specify the columns by selecting the corresponding check boxes.

   You can choose from the following columns: License Name, Device Count, Expiration Time, Key, Registered, Created By, and Created Time.

Register a License

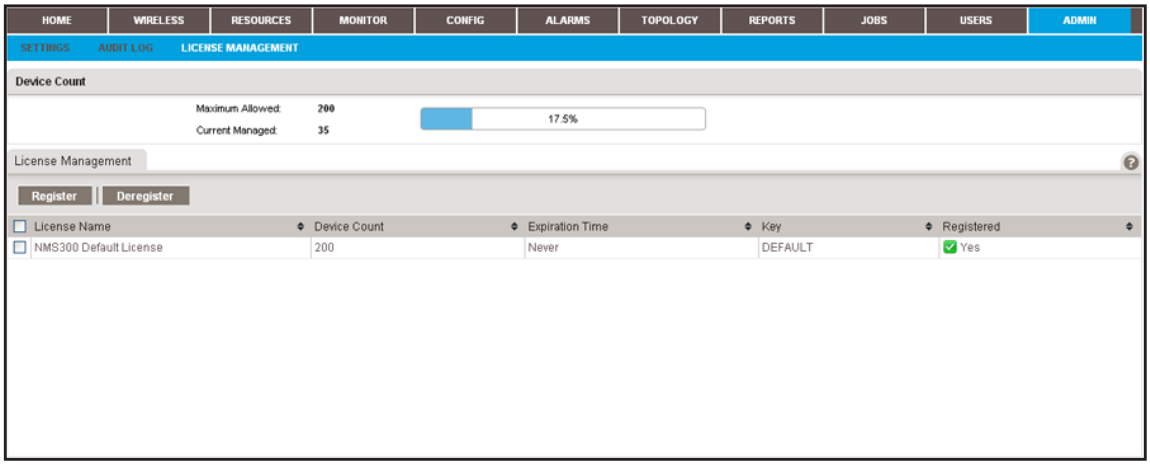
To register a license, you need a license key, and the NMS300 server must be connected to the Internet to connect to a NETGEAR license server.

➢ **To register a license:**

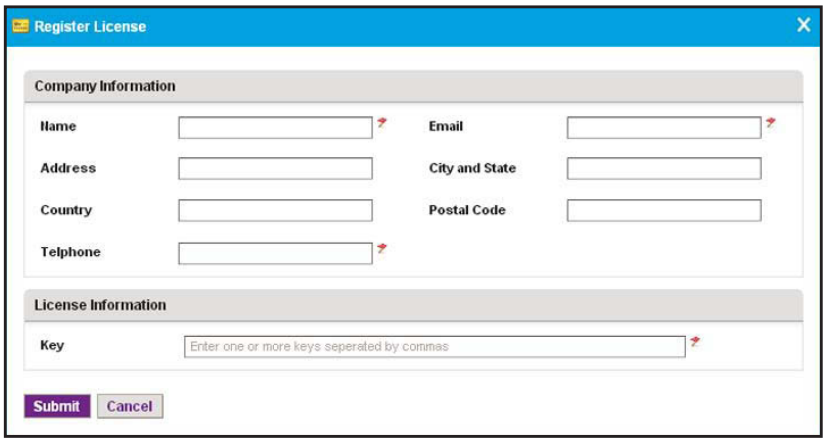
1. Log in to the application.

   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > LICENSE MANAGEMENT**.



3. Select the license.
4. Click the **Register** button.



5. In the Company Information section, enter your information.

   You must enter information in the **Name**, **Email**, and **Telephone** fields.

6. In the License Information section, enter the license key in the **Key** field.

   You must enter a single license key.

7. Click the **Submit** button.

   The license is registered with a NETGEAR license server. After successful registration, the license is added to the License Registration table. The license is tied to the MAC address of the NMS300 server.

Deregister a License

You can deregister a license on one NMS300 server, transfer it to another NMS300 server, and reregister the license on the new NMS300 server. You cannot deregister the default license.

After you deregister a license, if the number of allowed devices falls below the number of managed devices, the application displays a wizard. To bring the number of managed devices within the limit of the number of allowed devices, the wizard lets you select devices from the currently managed list that you can delete from the application.

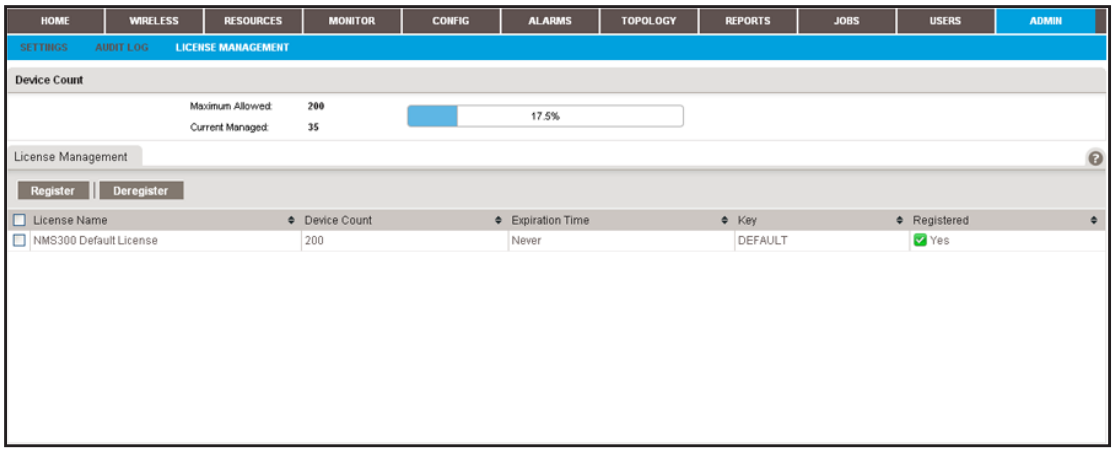
To deregister a license, the NMS300 server must be connected to the Internet to connect to a NETGEAR license server.

➢ **To deregister a license:**

1. Log in to the application.

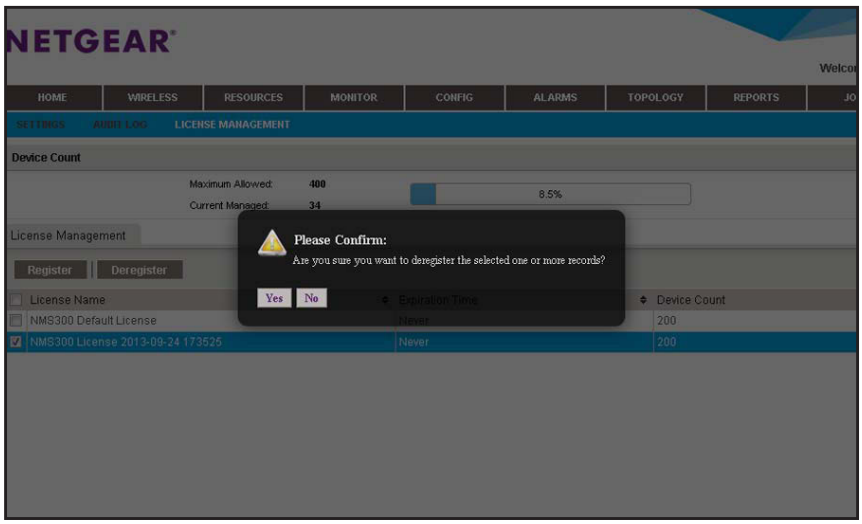
   For more information, see *Log In to the Application* on page 15.

2. Select **ADMIN > LICENSE MANAGEMENT**.



3. Select the license.
4. Click the **Deregister** button.

   A pop-up confirmation screen displays.



5. Click the **Yes** button.

   The license is removed from the License Management table and deregistered.

Technical Specifications

A

Hardware and software requirements

Item	Specification
System architecture	• B/S-based multitiered system
Browser support (HTTP and HTTPS)	• Internet Explorer 9 • Firefox 20.0.1 • Chrome 26.0.1410.64 m
OS support	• Windows Server 2003 (Standard, Enterprise, and Web), 32-bit and 64-bit • Windows Server 2008 (Enterprise) 32-bit and 64-bit • Microsoft Windows XP (Professional) 32-bit and 64-bit with SP3 or later • Microsoft Windows 7 (Professional, Enterprise, and Ultimate) 32-bit and 64-bit
VM support	• Support hypervisors include VMWare and other major ones such as Hyper-V and XenServer
Standard server requirement (for 200 devices)	• 2.8 GHz dual-core CPU • 4 G RAM (32-bit OS) or 8 G RAM (64-bit OS) • 20 G HD (free space) • Static IP
Standard client requirement	• 2 GHz CPU • 2 G RAM • 3 G HD (free space)
Installation	• Server is installed through an automated GUI-based installer • Single server deployment • Client is web-based and no installation is required
Language support	• English • Support other languages through internationalization
Management interface support	• SNMP (v1, v2c, v3) • TFTP • Telnet/HTTP/HTTPS • Web management interface

Item	Specification
Supported devices	See *Compatible Devices* on page 10
DB	MySQL (v5.5)

Device Details

B

Device details that you can display

You can view many details for a device and its interfaces. For information about how to view details, see *View Device Details and Interface Details*.

The detailed information that the application can provide depends on the type of device. The Devices table can list the following devices in the Device Type column:

- **Switch**. For information about the available details, see *Switch Details* on page 228 and *Interface Details* on page 235.
- **Firewall**. For information about the available details, see *Firewall Details* on page 229.
- **Standalone AP**. For information about the available details, see *Standalone AP Details* on page 229.
- **Controller-Managed AP**. For information about the available details, see *Controller-Managed AP Details* on page 231.
- **Wireless Controller**. For information about the available details, see *Wireless Controller Details* on page 232 and *Interface Details* on page 235.
- **WMS**. For information about the available details for a wireless management system, see *Wireless Controller Details* on page 232.
- **Router**. For information about the available details, see *Wireless Controller Details* on page 232 and *Interface Details* on page 235.
- **Unknown**. For information about the available details for an unknown device, see *Wireless Controller Details* on page 232.

Switch Details

The following table lists the dashboard options and widgets or tables that are available for a switch.

Table 4. Detailed information available for a switch

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Average CPU and Memory Utilization (Today)
	Inventory Information
	Min/Max/Average Response Time
	Latest 10 Alarms
	CPU
	Top 10 Interface by Traffic (Today)
	Memory
	Latest 10 Config Backups
Interface List	Interface List **Note:** For more information, see *Table 12* on page 235.
Traffic Monitor	IP Traffic Monitor
	ICMP Traffic Monitor
	TCP Traffic Monitor
	UDP Traffic Monitor
	SNMP Traffic Monitor
Bandwidth Monitor	Received Bytes (KB) Real-time Chart
	Transmitted Bytes (KB) Real-time Chart
	Selected interfaces
Config Files	Config File Backup List
Credential	Authentication Association

Firewall Details

The following table lists the dashboard options and widgets or tables that are available for a firewall.

Table 5. Detailed information available for a firewall

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Latest 10 Alarms
	Top 10 Interface by Traffic (Today)
	Latest 10 Config Backups
Config File	Config File Backup List
Credential	Authentication Association

Standalone AP Details

The following table lists the dashboard options and widgets or tables that are available for a standalone AP)

Table 6. Detailed information available for a standalone AP

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Average CPU and Memory Utilization (Today)
	Inventory Information
	Min/Max/Average Response Time
	Wireless Info (Current)
	CPU
	Latest 10 Alarms
	Memory
	Latest 10 Config Backups

Table 6. Detailed information available for a standalone AP (continued)

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table	
Radios and Network	2.4 GHz	Radio and networks
		SSID and authentication information
	5 GHz	Radio and networks
		SSID and authentication information
Client List	Active Client List **Note:** For more information, see *Monitor Wireless Clients and View Client Details* on page 80.	
Top 10	Top 10 Client by Traffic (Current)	
	Top 10 SSID by Client Count (Current)	
	Top 10 SSID by Traffic (Today)	
Wireless Monitor	WLAN Utilization	
	Monitor per SSID	Wireless Client Count By SSID
		Wireless Traffic (Received and Transmitted) By SSID
		Wireless Frames (Received and Transmitted) By SSID
	Monitor per Radio	Wireless Traffic (Received and Transmitted) By Radio
		Wireless Client Count By Radio
		Wireless Packets (Received and Transmitted) By Radio
Wired Monitor	Total Traffic	Wired Received/Transmitted Bytes
		Wired Received/Transmitted Packets
	Traffic by Protocol	IP Traffic Monitor
		ICMP Traffic Monitor
		TCP Traffic Monitor
		UDP Traffic Monitor
		SNMP Traffic Monitor
Config Files	Config File Backup List	
Credential	Authentication Association	

Controller-Managed AP Details

The following table lists the dashboard options and widgets or tables that are available for a controller-managed AP.

Note: Because of the nature of controller-managed APs, the application can provide only limited information for controller-managed APs, compared to standalone APs.

Table 7. Detailed information available for a controller-managed AP

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table	
Controller Managed AP Details	General Information	
	Latest 10 Alarms	
Radios and Network	2.4 GHz	Radio and Networks
		SSID and authentication information
	5 GHz	Radio and Networks
		SSID and authentication information
Client List	Active Client List **Note:** For more information, see *Monitor Wireless Clients and View Client Details* on page 80.	
Top 10	Top 10 Client by Traffic (Current)	
	Top 10 SSID by Client Count (Current)	
AP Monitor	Monitor per SSID	Wireless Client Count By SSID
	Monitor per Radio	Wireless Client Count By Radio

Wireless Controller Details

The following table lists the dashboard options and widgets or tables that are available for a wireless controller.

Table 8. Detailed information available for a wireless controller

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table	
Controller Details	General Information	
	Average Response Time and Packet Loss (Today)	
	Min/Max/Average Response Time	
	Inventory Information	
	Latest 10 Alarms	
	Latest 10 Config Backups	
Profiles	802.11b/bg/ng	Profiles
	802.11a/na	Profiles
Top 10	Top 10 Client by Traffic (Current)	
	Top 10 Controller Managed AP by Client Count (Current)	
	Top 10 SSID by Client Count (Current)	
AP List	Access Points	
Client List	Active Client List **Note:** For more information, see *Monitor Wireless Clients and View Client Details* on page 80.	
Interface List	Interface List **Note:** For more information, see *Table 12* on page 235.	
Traffic Monitor	IP Traffic Monitor	
	ICMP Traffic Monitor	
	TCP Traffic Monitor	
	UDP Traffic Monitor	
	SNMP Traffic Monitor	
Bandwidth Monitor	Received Bytes (KB) Real-time Chart	
	Transmitted Bytes (KB) Real-time Chart	
	Selected interfaces	

Table 8. Detailed information available for a wireless controller (continued)

Dashboard Menu Option	Dashboard Submenu Option, Widget, or Table
Config File	Config File Backup List
Credential	Authentication Association

Wireless Managements System Details

The following table lists the dashboard options and widgets or tables that are available for a wireless management system (WMS).

Table 9. Detailed information available for a WMS

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Inventory Information
	Latest 10 Alarms
	Latest 10 Config Backups
Interface List	Interface List **Note:** For more information, see *Table 12* on page 235.
Config Files	Config File Backup List
Credential	Authentication Association

Router Details

The following table lists the dashboard options and widgets or tables that are available for a router.

Table 10. Detailed information available for a router

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Inventory Information
	Top 10 Interface by Traffic (Today)
	Latest 10 Alarms
Interface List	Interface List **Note:** For more information, see *Table 12* on page 235.
Traffic Monitor	IP Traffic Monitor
	ICMP Traffic Monitor
	TCP Traffic Monitor
	UDP Traffic Monitor
	SNMP Traffic Monitor

Unknown Device Details

The following table lists the dashboard option and widgets that are available for an unknown device.

Table 11. Detailed information available for an unknown device

Dashboard Menu Option	Widget or Table
Device Details	General Information
	Average Response Time and Packet Loss (Today)
	Min/Max/Average Response Time
	Latest 10 Alarms

Interface Details

The interface details can display for switches, wireless controllers, wireless management systems, and routers. The following table lists the dashboard options and widgets or tables that are available for an interface.

Table 12. Detailed information available for an interface

Dashboard Menu Option	Widget or Table
Interface Details	General Information
	Traffic Information
	Latest 10 Alarms
Monitor Data	Interface Received/Transmitted Bytes
	Interface Received/Transmitted Packets
	Interface Utilization (%)
	Interface Traffic Rate (bps)
	Interface Inbound/Outbound Error Packets
	Interface Inbound/Outbound Discards
Network Details	VLAN Membership
	Forwarding Database
	Common STP Port Status